EXHIBIT D

PLR 4-3(b) –Microsoft's Listing of Intrinsic and Extrinsic Evidence

Each claim phrase incorporates the Intrinsic and Extrinsic support of the individual terms within it.

Claim Term	MS Construction
access, accessed, access to, accessing 193.15, 193.19, 912.8, 912.35, 861.58, 683.2, 721:34	Intrinsic: - "These rights govern use of the VDE object 300 by that user or user group. For instance, the user may have an "access" right, and an "extraction" right, but not a "copy" right." ('193 159:32)[1] - ('193 82:27-45); ('193 109:53-57); ('193 118:17-31); (193 139:60-140:6); ('193 148:55-58); ('193 183:12-29); ('193 188:59-67); ('193 192:2-24) Extrinsic:[2] Access (n): 2. The use of an access method. 3. The manner in which files or data sets are referred to by the computer. 5. In computer security, a specific type of interaction between a subject and an object that results in the flow of information from one to the other. (IBM)[3] Access (n.): 1. In access control, a specific type of interaction between a subject and an object that results in the flow of information from on to the other 3. In computing, the manner in which files or data sets are referred to by a computer (Longley)[4] Access(ing) (v.): 1. To obtain the use of a computer resource. 4. To obtain data from or to put data in storage. (IBM)
addressing 861.58	Intrinsic: "Load modules 1100 in the preferred embodiment are modular and "code pure" so that individual load modules may be reenterable and reusable. In order for components 690 to be dynamically updatable, they may be individually addressable within a global public name space." ('193 86:49-53) Extrinsic: Addressing (v): 1. A character or group of characters that identifies a register, a particular part of storage, or some other data source or destination. 4. A name, label, or number identifying a location in storage, a device in a system or network, or any other data source. 5. In data communication, the unique code assigned to each device or workstation connected to a network.(IBM) Addressing (n.): 1. In computing, a character or group of characters that identifies a register, a particular part of storage, or some other data source or destination 2. In computing, to refer to a device or an item of data by its address. (Longley) Addressing (v): 1. In computing, the assignment of addresses to the instructions of a program 2. In communications, the means whereby the originator or control station selects the unit to which it is going to send a message (Longley)
allowing, allows 912.35, 193.1, 193.11, 193.15, 193.19	Intrinsic: - SN 08/780,545 ('912): 10/29/98 amendment to claim 211 (issued claim 35) "necessary in order to gain" to "allowing" - VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:51-56)

[1] Citations to the '193 Patent are representative of citations to the text and drawings of the "Big Book" application also published in the '891, '900, and '912 Patents. Emphasis is added unless otherwise noted.
[2] Extrinsic evidence is cited herein without waiver of any kind, including relevance or probative value.
[3] "IBM" herein refers to IBM Dictionary of Computing, 10th ed., 1983.
[4] "Longley" herein refers to Longley, D., et al, Information Security: Dictionary of Concepts, Standards, and Terms, 1992

Claim Term	MS Construction
	- VDE is a secure system for regulating electronic conduct and commerce. Regulation is ensured by control information put in place by one or more parties. ('193 6:33-34) - VDE ensures that certain prerequisites necessary for a given transaction to occur are met. ('193 20:27-28) - ('193 309:10-16); ('193 15:41-46); ('193 17:22-28); ('193 303:67-304:1) Extrinsic: Least privilege: Each user and each program should operate using the fewest privileges possible. In this way, the damage from an inadvertent or malicious attack is minimized. (Pfleeger)[5]
arrangement 721.34	See also phrases of use in 721.34. Intrinsic: An important part of VDE provided by the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other electronic appliance, or network. ('193 48:66)
aspect 900.155, 912.8, 861.58, 683.2	See also phrases of use in 900.155, 912.8, 861.58, 683.2. Extrinsic: Aspect: The qualification of a descriptor. (IBM)
associated with 912.8, 193.1, 193.11, 193.15, 683.2	Intrinsic: - "VDEF load modules, associated data, and methods form a body of information that for the purposes of the present invention are called "control information." VDEF control information may be specifically associated with one or more pieces of electronic content and/or it may be employed as a general component of the operating system capabilities of a VDE installation." ('193 18:36-42) - "As mentioned above, virtual distribution environment 100 "associates" content with corresponding "rules and controls," and prevents the content from being used or accessed unless a set of corresponding "rules and controls" is available." ('193 57:18-22) - "This "lookup" mechanism permits electronic appliance 600 to associate, in a secure way, VDE objects 300 with PERCs 808, methods 1000 and load modules 1100." ('193 153:35-38) - ('193 55:39-45); ('193 142:50-52); ('193 57:30-33); ('861 1:50-53) Extrinsic: Association: In the Open Systems Interconnection reference model, a cooperative relationship between two peer entities, supported by the exchange of protocol control information using the services of the next lower layer. (IBM)
authentication 193.15	Intrinsic: - A certification key pair may be used as part of a "certification" process for PPEs 650 and VDE electronic appliances 600. This certification process in the preferred embodiment may be used to permit a VDE electronic appliance to present one or more "certificates" authenticating that it (or its key) can be trusted. As described above, this "certification" process may be used by one PPE 650 to "certify" that it is an authentic VDE PPE, it has a certain level of security and capability set (e.g., it is hardware based rather than merely software based), etc. ('193 212:66-213:15) - "One of the functions SPU 500 may perform is to validate/authenticate VDE objects 300 and other items. Validation/authentication often involves comparing long data strings to determine whether they compare in a predetermined way." ('193 67:56-60)

[5] "Pfleeger" herein refers to Pfleeger, Security in Computing (1989).

Claim Term	MS Construction
	- ('683 17:20-27); ('683 52:56-60); ('193 112:46-61) Extrinsic: Authentication: 1. In computer security, verification of the identity of a user or the user's eligibility to access an object. 2. In computer security, verification that a message has not been altered or corrupted. 3. In computer security, a process used to verify the user of an information system or protected resources. 4. A process that checks the integrity of an entity. (IBM) Authentication: 1. In data security, the act of determining that a message has not been changed since leaving its point of origin. 4. In computer security, the act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information (Longley)
authorization information, authorized, not authorized 193.15, 193.19	Intrinsic: - See "allow." Several independent comparisons may be used to ensure there has been no unauthorized substitution. For example, the public and private copies of the element ID may be compared to ensure that they are the same, thereby preventing gross substitution of elements. In addition, a validation/correlation tag stored under the encrypted layer of the loadable element may be compared to make sure it matches one or more tags provided by a requesting process. This prevents unauthorized use of information. ('193 87:47-55) "using said authorization information to gain access to or make at least one use of said first digital file" ('193 Claim 19) Extrinsic: Authorization: 1 In computer security, the right granted to a user to communicate with or make use of a computer system. 2. An access right. 3. The process of granting a user either complete or restricted access to an object, resource, or function. (IBM) Authorization: (1) In access control, the granting to a user, a program, or a process the right of access. (2) In operations, the right given to a user to communicate with or make use of a computer system or stored data. 3. The privilege granted to an individual by a designated official to access information based upon the individual's clearance and need-to-know. (Longley) Authorization: "A system control feature that requires specific approval before the processing can take place." (Webster's New World Dictionary of Computer Terms, 4th ed., 1992)
budget control; budget 193.1	Intrinsic: - ""Budgets" 308 shown in FIG. 5B are a special type of "method" 1000 that may specify, among other things, limitations on usage of information content 304, and how usage will be paid for. Budgets 308 can specify, for example, how much of the total information content 304 can be used and/or copied. The methods 310 may prevent use of more than the amount specified by a specific budget." ('193 59:19-25) (See also Fig. 5B) - "For example, consider the case of a security budget. One form of a typical budget might limit the user to 10Mb of decrypted data per month." ('193 265:9-11) - "An example of the process steps used for the move of a budget record might look something like this: 1) Check the move budget (e.g., to determine the number of moves allowed) ('193 265:24-27) - "BUDGET method 408 may store budget information in a budget UDE" ('193 182:25-26) - "In the preferred embodiment, a "method" 1000 is a collection of basic instructions, and information related to basic instructions, that provides context, data, requirements and/or relationships for use in performing, and/or preparing a perform, basic instructions in relation to the operation of one or more electronic appliances 600." ('193 85:43-48; repeated essentially at '193 136:20-25) - BUDGET method 408 may result in a "budget remaining" field in a budget UDE being decremented

Claim Term	MS Construction
	by an amount specified by BILLING method 406. ('193 182:22-30) - ('193 58:27-34); ('193 187:48-50); ('193 235:39-42); ('193 143:63 - 144:14); ('193 265:44-51) Extrinsic: Budget: A budget is the control mechanism for a meterable feature. A budget provides an upper limit for the volume of a meterable feature that a user (client) may use. Budgets consist of two values: a ceiling limit on use and an increment value that is added to the associated meter when a meterable event occurs. Budgets may be stand-alone or cascaded. A stand-alone budget only increments the meters for itself, while a cascaded budget can increment many meters from a single meterable event. A budget consists of an identification sextet, a descriptive area that describes the budget (cascade budget tuple and other miscellaneous flags), and a series of budget tuples. Each budget tuple consists of a budget and the increment value. It should be noted that a budget may be specified in meterable events or in dollars, based on the type of meter the budget will be compared against. (VDE ROI Device v1.0a, 9 Feb 1994, IT00008582) Control: The determination of the time and order in which the parts of a data processing system and the devices that contain those parts perform the input, processing, storage, and output functions. (IBM) Budget Object: A governed element that defines the consumer's ability to provide payment using a specific payment type. ((ITG, 1997-1998, ML00012B)[6] Budget Object: *An InterTrust system object* that defines the consumer's ability to provide payment using a specific payment type. ((emphasis added) IT System Developers Kit, 1997, TD00298C) Budget: A control mechanism that limits operations on content based on billed amounts that can maintain a budget trail. A budget may be financially based (e.g., a number of dollars available for purchasing content use) or abstract (e.g. a total number of permitted usages). VTG, 3/7/95, IT00709617) Budget: *A fixed quantity of money, time, etc. against which the cost of operation is charged. Budget activities usually also involve reporting. ((ITG, 8/21/95, IT0032371) Control: Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node. ((ITG, 5/12/95, IT00028293) Control: A business rule that governs the use of content. ((ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply to either a control program or a control set. ((ITG, 1997-2000, ML00012D) Control: **Control Element*: A data structure that giverns (*sic)* the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). **Control mechanism*: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. **Control Parameter:* A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. ((ITG, 3/7/1995, IT00709618, see footnote 2)
can be 193.1	Intrinsic: VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content

[6] "(ITG" herein is a generic reference to several InterTrust glossaries that are further identified by Bates number or IT document number.

Claim Term	MS Construction
	users." ('193 4:51-56) - VDE is a secure system for regulating electronic conduct and commerce. Regulation is ensured by control information put in place by one or more parties. ('193 6:33-35) - It also employs a software object architecture for VDE content containers that carries protected content and may also carry both freely available information (e.g, summary, table of contents) and secured content control information which ensures the performance of control information. ('193 15:41-46) - Because of the breadth of issues resolved by the present invention, it can provide the emerging "electronic highway" with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions. ('193 17:22-28) - VDE ensures that certain prerequisites necessary for a given transaction to occur are met. ('193 20:27-28) - "support "launchable" content, that is content that can be provided by a content provider to an end-user, who can then copy or pass along the content to other end-user parties without requiring the direct participation of a content provider to register and/or otherwise initialize the content for use." ('193 24:57-62) - "For example, budget process 408 may limit the number of times content may be accessed or copied, or it may limit the number of pages or other amount of content that can be used based on, for example, the number of dollars available in a credit account." ('193 58:28-32) - "Budgets 308 can specify, for example, how much of the total information content 304 can be used and/or copied. The methods 310 may prevent use of more than the amount specified by a specific budget." ('193 59:22-25) - "As an alternative example, a creator may allow moving of usage rights by a distributor to half a dozen subdistributors, each of whom can distribute 10,000 copies, but with no redistribution rights being allowed to be allocated to subdistributors' (redistributors') customers. ... Content providers and other contributors of control information have the ability through the use of permissions records and/or component assemblies to control rights other users are authorized to delegate in the permissions records they send to those users, so long as such right to control one, some, or all such rights of other users is either permitted or restricted (depending on the control information distribution model)." ('193 269:34-49) "In such systems, because document content can be freely copied and manipulated, it is not possible to determine where document content has gone, or where it came from." ('193 281:33-36)
capacity 683.2	Intrinsic: "Some items may be too large to store within container 302." ('193 58:54-55) ('193 243:23 – 244:48) Extrinsic: Capacity: See channel capacity, storage capacity.(IBM) Channel Capacity: The measure of the ability of a given channel subject to specific constraints to transmit messages from a specified message source expressed as either the maximum possible mean transinformation content per character or the maximum possible average transinformation rate, which can be achieved with an arbitrary small probability of errors by use of an appropriate code. (IBM) Storage capacity: The amount of data that can be contained in a storage device measured in binary characters, bytes, words, or other units. For registers, the term "register length" is used with the same meaning. Synonymous with storage size. (IBM)
clearinghouse	Intrinsic:

Claim Term	MS Construction
193.19	- "Distribution involves three types of entity. Creators usually are the source of distribution. They typically set the control structure "context" and can control the rights which are passed into a distribution network. Distributors are users who form a link between object (content) end users and object (content) creators. They can provide a two-way conduit for rights and audit data. Clearinghouses may provide independent financial services, such as credit and/or billing services, and can serve as distributors and/or creators. Through a permissions and budgeting process, these parties collectively can establish fine control over the type and extent of rights usage and/or auditing activities." ('193 267:34-45) - "Payment credit or currency may then be automatically communicated in protected (at least in part encrypted) form through telecommunication of a VDE container to an appropriate party such as a clearinghouse, provider of original property content or appliance, or an agent for such provider (other than a clearinghouse)." ('193 36:64-37:3) "if appropriate credit (e.g. an electronic clearinghouse account from a clearinghouse such as VISA or AT &T) is available" ('193 25:22-24) Extrinsic: Clearinghouse: *A facility that receives reports of content use and in turn reports payments and usage to content creators and distributors. (ITG, 8/21/95, IT00032372, TD00068B)
compares, comparison 900.155	Intrinsic: "ROS 602 also provides a tagging and sequencing scheme that may be used within the loadable component assemblies 690 to detect tampering by substitution. Each element comprising a component assembly 690 may be loaded into an SPU 500, decrypted using encrypt/decrypt engine 522, and then tested/compared to ensure that the proper element has been loaded. Several independent comparisons may be used to ensure there has been no unauthorized substitution. For example, the public and private copies of the element ID may be compared to ensure that they are the same, thereby preventing gross substitution of elements." ('193 87:41-51) Extrinsic: Compare: 1. To examine two items to discover their relative magnitudes, their relative positions in an order or in a sequence, or whether they are identical in given characteristics. 2. To examine two or more items for identity, similarity, equality, relative magnitude, or order in a sequence.(IBM) Comparison: The process of examining two or more items for identity, similarity, equality, relative magnitude, or for order in sequence. (IBM)
component assembly 912.8, 912.35	Intrinsic: - "Many such load modules are inherently configurable, aggregatable, portable, and extensible and singularly, or in combination (along with associated data), run as control methods under the VDE transaction operating environment." ('193 25:48-52) - ('193 77:12-27); ('193 83:11-22); ('193 181:20-21); ('193 272:29-36) - "Components 690 are preferably designed to be easily separable and individually loadable. ROS 602 assembles these elements together into an executable component assembly 690 prior to loading and executing the component assembly (e.g., in a secure operating environment such as SPE 503 and/or HPE 655)." ('193 83:43-48) - ('193 83:23); ('193 85:21-29 see '193 170:2-4); ('193 86:51-52); ('193 87:41-62); ('193 109:24-45); ('193 115:65-116:4); ('193 116:30-34); ('193 185:42-46) Extrinsic: Component: 1. Hardware or software that is part of a functional unit. 2. A functional part of an operating system. 3. A set of modules that performs a major function within a system. (IBM) Component: In data communications, a device or set of devices, consisting of hardware, along with its

Claim Term	MS Construction
	firmware, and or software that performs a specific function on a computer communications network. A Component is a part of a larger system, and may itself consist of other components. (Longley) "Thus, PERC 808 in effect contains a "list of assembly instructions" or a "plan" specifying what elements ROS 602 is to assemble together into a component assembly and how the elements are to be connected together. PERC 808 may itself contain data or other elements that are to become part of the component assembly 690." ('193 85:30-39)
contain, contained, containing 683.2, 912.8, 912.35	Intrinsic: - "Container 300y may contain and/or reference rules and control information 300y(1) that specify the manner in which searching and routing information use and any changes may be paid for." ('193 241:36-39) - "Each logical object structure 800 may also include a "private body" 806 containing or referencing a set of methods 1000 (i.e., programs or procedures) that control use and distribution of the object 300." ('193 128:25-28) - "Therefore, stationary object structure 850 does not contain a permissions record (PERC) 808; rather, this permissions record is supplied and/or delivered separately (e.g., at a different time, over a different path, and/or by a different party) to the appliance/installation 600. ('193 130:18-22) - "The content portion of a logical object may be organized as information contained in, not contained in, or partially contained in one or more objects." ('193 127:8-19) - "Therefore, stationary object structure 850 does not contain a permissions record (PERC) 808; rather, this permissions record is supplied and/or delivered separately (e.g., at a different time, over a different path, and/or by a different party)" ('193 130:18) - ('193 58:49-58); ('193 86:47-48); ('193 87:3-6); ('193 130:63-64); ('193 136:32-34); ('193 241:36-39); ('683 54:29-37) See also prior art referred to the relevant InterTrust patent file histories, e.g. U.S. Patent 5,715,403 Extrinsic: "Container: A contains protected *content*, which is divided into one or more *atomic elements*, and, optionally, *PERCs* governing the *content* and may be manipulated only as specified by a *PERC.*" (ITG, 4/6/95, IT00028206, see footnote 2 and 4) "Container: A packaging mechanism, consisting of: *One or more Element-derived components. *An organization mechanism which provides a unique name within a flat namespace for each of the components in a Container." (ITG, 5/12/95, IT00028293) "Container: A protected digital information storage and transport mechanism for packaging content and control information." (ITG, 8/21/95, IT00032372, TD00068B) Container: A collection of content and control-related information. (IT VDE Container Overview, 2/10/95, IT00051228, ETM-9999 Version 0.21) Contain: In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers. (Longley, Information Security :Dictionary of Concepts, Standards, and Terms (1992) USP 5,369,702 Que's Computer Programmer's Dictionary ("Que") ("A dynamic data structure, the elements of which are arbitrary data items whose type is not known when the program is written." Dictionary of Computer Science Engineering and Technology (2001) ("Abstract data type storing a collection of objects (elements)") IT00037-44, IT002734-39, IT004188-96, IT0031572-85, IN00075960, IT00703055-71, IT0052146-64, IN00441189-224, IN0075983-87 See also Microsoft PLR 4-2 Exhs. E & F as revised, and InterTrust's Rule 30(b)(6) testimony.

Claim Term	MS Construction
control (n.) 193.1, 193.11, 193.15, 193.19, 891.1	Intrinsic: - "Claims ... are allowable over the prior art of record. The instant claims provide for first and second entity or control or procedure or executable code that are separately, remotely and different from each to combine or process or execute an operation or procedure based on at least first and second control or procedure or executable code in an electronic appliance or secure operating environment or third party different and remote from the first and second entity or control or procedure or executable code." 08/964,333 ('891), Office Action, 09/22/98, p. 3 (MSI028945) - "The virtual distribution environment 100 prevents use of protected information except as permitted by the "rules and controls" (control information)." ('193 56:26) - "As mentioned above, virtual distribution environment 100 "associates" content with corresponding "rules and controls," and prevents the content from being used or accessed unless a set of corresponding "rules and controls" is available." ('193 57:18-22) - "at least one rule and/or control associated with the software agent that governs the agent's operation." ('193 241:2-3) - "In this example control information may include one or more component assemblies that describe the articles within such a container (e.g. one or more event methods referencing map tables and/or algorithms that describe the extent of each article)." ('193 309:5-9) - ""Even if a consumer has a copy of a video program, she cannot watch or copy the program unless she has "rules and controls" that authorize use of the program. She can use the program only as permitted by the "rules and controls." ('193 53:60-63) - "A control set 914 contains a list of required methods that must be used to exercise a specific right (i.e., process events associated with a right)." ('193 151:14-16) - "If necessary, trusted go-between 4700 may obtain and register any methods, rules and/or controls it needs to use or manipulate the object 300 and/or its contents (FIG. 122 block 4778)." ('683, sheet 188) See also prior art referred to the relevant InterTrust patent file histories. MSI026598-602, 26626-7, 26630-42; MSI 028808-11, 28846-52, 28728-62, 28857-58, 28944-97, 28953-56 Extrinsic: Control: The determination of the time and order in which the parts of a data processing system and the devices that contain those parts perform the input, processing, storage, and output functions. (IBM) "5. Control Notes . . . A Control must execute as a transaction . . . A Control may require pre-conditions – that is that one or more other Controls have been executed before the Control is executed. [] 7. Control Execution Flow The following pseudocode describes the approximate execution sequence for a View Control [] 8. Operation of a Control (Execution of "Rules and Consequences") . . ." (VDE Controls Notes, IT00051953-55) Control: A business rule that governs the use of content. (ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply to either a control program or a control set. (ITG, 1997-2000, ML00012D) Control: **Control Element*: A data structure that giverns (*sic)* the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). **Control mechanism*: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. **Control Parameter:* A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. (ITG, 3/7/1995, IT00709618, see footnote 2) Control: Defines rules and consequences for operations on a Property Chunk. A Control may be

Claim Term	MS Construction
	implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node.(ITG, 5/12/95, IT00028293) Control: A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc. (ITG, 8/21/95, IT00032373, TD00068B) Control: An object of the InterTrust Commerce Architecture that specifies business rules. Controls are applied at any time and at any point in the Chain of Handling and Control. InterTrust controls are dynamic, independent, and persistent. (ITG, 11/17/96, IT00035865, TD00189J) "Rules and Controls" means any electronic information that directs, enables, specifies, describes, and/or provides contributing means for performing or not-performing, permitted and/or required operations related to Content, including, for example, restricting or otherwise governing the performance of operations, such as, for example, Management of such Content. (License Agreement, InterTrust/Universal Music Group, 4/13/99, Exhibit 11 to InterTrust 30(b)(6)) "A set of control elements corresponding to all of the property elements of a property. There may be zero or more controls for a given property." (IT 28204) "Defines rules and consequences for operations on a Property Chunk . . . A single control applies to exactly one Property Chunk" (IT 28293) "CONTROL(S): Controls refer to the rules and consequences associated with DigiBox containers. Controls may be applied dynamically. . ." (IT 35961) "CONTROL: The rules associated with a governed entity such as a DigiBox container, property, or another control . . . applied dynamically. InterTrust controls are dynamic, independent, and persistent." (IT 35920) ". . . controls implement business rules" (IT 35892) Webster's New World Dictionary of Computer Terms, 4th Ed. (1992) ("The function of performing required operations when certain specific conditions occur or when interpreting and acting upon instructions."); IT00125, IT31410-14, IT703083-89, IT51721-26, IT00735936 (key), IT51956 et seq., IN0075983-87, IN0075989-93; The Dictionary of Computing & Digital Media (1999) (control card) See also Microsoft PLR 4-2 Exhs. E & F as revised, and InterTrust's Rule 30(b)(6) testimony.
controlling, control (v.) 861.58, 193.1	Intrinsic: - "ROS 602 includes software intended for execution by SPU microprocessor 520 for, in part, controlling usage of VDE related objects 300 by electronic appliance 600. As will be explained, these SPU programs include "load modules" for performing basic control functions." ('193 66:5-8) - "VDE prevents many forms of unauthorized use of electronic information, by controlling and auditing (and other administration of use) electronically stored and/or disseminated information." ('193 11:60-63) - ('193 15:41-46); ('193 20:27-28); ('193 56:26-28); ('193 57:18-22) ('193 4:51-56); ('193 6:33-35); ('193 15:41-46); ('193 17:22-28); ('193 20:27-28) Extrinsic: Control: The determination of the time and order in which the parts of a data processing system and the devices that contain those parts perform the input, processing, storage, and output functions. (IBM) Control: In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers. (Longley) Control: A business rule that governs the use of content. (ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply

Claim Term	MS Construction
	to either a control program or a control set. (ITG, 1997-2000, ML00012D) Control: **Control Element*: A data structure that giverns (*sic*) the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). **Control mechanism*: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. **Control Parameter:* A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter, a creator using that mechanism could alter the parameter but not change the mechanism itself. (ITG, 3/7/1995, IT00709618, see footnote 2) Control: Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node. (ITG, 5/12/95, IT00028293) Control: A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc. (ITG, 8/21/95, IT00032373, TD00068B)
copied file 193.11	Intrinsic: Extrinsic: Copy: A product of a document copying process.(IBM)
copy, copied, copying 193.1, 193.11, 193.15, 193.19	Intrinsic: - "These rights govern use of the VDE object 300 by that user or user group. For instance, the user may have an "access" right, and an "extraction" right, but not a "copy" right." ('193 159:23-26) - "At the same time, electronic testing will allow users to receive a copy (encrypted or unencrypted) of their test results when they leave the test sessions." ('193 319:12-15) - ('193 129:3-8); ('193 claim 60); ('193 53:60-62); ('193 131:65-132:1) Extrinsic: Copy: A product of a document copying process.(IBM)
copy control 193.1	Intrinsic: - "If the user's budget permits the extraction ("yes" exit to decision block 2088), then the EXTRACT method 2080 creates a copy of the extracted object with specified rules and control information (block 2094). In the preferred embodiment, this step involves calling a method that actually controls the copy." ('193 194:36-42) Extrinsic: Copy Control: In the 3800 Printing Subsystem, the functions that determine the number of copies to be printed for each data set, and which copies will be printed with a forms overlay or have copy modification. (IBM) Control: A business rule that governs the use of content. (ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply to either a control program or a control set. (ITG, 1997-2000, ML00012D) Control: **Control Element*: A data structure that giverns (*sic*) the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). **Control mechanism*: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. **Control Parameter:* A

Claim Term	MS Construction
	data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. (ITG, 3/7/95, IT00709618, see footnote 2) Control: Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node.(ITG, 5/12/95, IT00028293) Control: A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc. (ITG, 8/21/95, IT00032373, TD00068B)
data item 891.1	Extrinsic: Data Item: 1. The smallest unit of named data that has meaning in the schema or subschema. 2. A unit of data, either a constant or a variable, to be processed. 3. In the AIX operating system, a unit of data to be processed that includes constants, variable, or array elements, and character substrings. 6. Synonymous with host variable. (IBM) Data Item: In databases, the smallest unit of data that has independent meaning. (Longley) Item List: A list of data included with various objects. Item lists take two forms. When they are first created, they are in the form of lists that contain one or more data items. When you are finished creating the list, you convert the list to a blob, which is a set of raw bits that store the data in a compact way. To retrieve items from the item list, you use the Interoperability Library item list functions, which convert the blob back to its interpreted list form and allow you to inspect the data items. (ITG, 1997-1998, ML00012B) Data Item: An Element-derived bag of bits. (e.g., budget , meter, etc.) (ITG, 5/12/95, IT00028293)
derive, derives 900.155	Intrinsic: "Such control information can continue to manage usage of container content if the container is "embedded" into another VDE managed object, such as an object which contains plural embedded VDE containers, each of which contains content derived (extracted) from a different source." ('193 28:60-65) Extrinsic:
descriptive data structure 861.58	Intrinsic: "The descriptive data structure can be used as a "template" to help create, and describe to other nodes, rights management data structures including being used to help understand and manipulate such rights management data structures." ('861 5:43-46) "Claims [1,10,25,26] are rejected under 35 U.S.C. 102(b) as being clearly anticipated by the common and decades-old practice of using database schema to describe the structure of a database which requires password/identifications for access. ... Claims [1-17,25-26] are rejected under 35 U.S.C. 102(a) as being anticipated by Anderson et al (Anderson), USP 5,537,526, Method and Apparatus for Processing a Display Document Utilizing a System Level Document. The claims are rejected on the basis of the correspondence between the teachings of Anderson and the elements of the claims as follows: As to claim 1 (and 10), the TabstractModel 502 is a machine readable, abstract descriptive data structure which interoperates with Tmodels 506 (TM), and TmodelSurrogates 504 (TMS). ... These models are clearly data structures, and while they can be of many types, the data they manage can include restrictions that correspond to rights management." (08/805,804 ('861), Office Action, 06/25/98, p. 2-3) - "The above-referenced Ginter et al. patent specification describes, by way of non-exhaustive

Claim Term	MS Construction
	example, "templates" that can act as a set (or collection of sets) of control instructions and/or data for object control software. See, for example, the "Object Creation and Initial Control Structures," "Templates and Classes," and "object definition file," "information" method and "content" methods discussions in the Ginter et al. specification. The described templates are, in at least some examples, capable of creating (and/or modifying) objects in a process that interacts with user instructions and provided content to create an object. Ginter et al. discloses that templates may be represented, for example, as text files defining specific structures and/or component assemblies, and that such templates—with their structures and/or component assemblies--may serve as object authoring and/or object control applications. Ginter et al. says that templates can help to focus the flexible and configurable capabilities inherent within the context of specific industries and/or businesses and/or applications by providing a framework of operation and/or structure to allow existing industries and/or applications and/or businesses to manipulate familiar concepts related to content types, distribution approaches, pricing mechanisms, user interactions with content and/or related administrative activities, budgets, and the like. This is useful in the pursuit of optimized business models and value chains providing the right balance between efficiency, transparency, productivity, etc. The present invention extends this technology by providing, among other features, a machine readable descriptive data structure for use in association with a rights management related (or other) data structure such as a *secure container*." ('861 4:65) - "For example, the FIG. 2A example descriptive data structure headline definition 202a does not specify a particular headline (e.g., "Yankees Win the Pennant!"), but instead defines the location (for example, the logical or other offset address) within the container data structure 100a (as well as certain other characteristics) in which such headline information may reside." ('861 10:54-59); - "These descriptive data structure ("DDS") templates may be used to create containers." ('861 6:26-32); - "the descriptive data structure may be used in a creation process 302. The creation process 302 may read the descriptive data structure and, in response, create an output file 400 with a predefined format such as, for example, a container 100 corresponding to a format described by the descriptive data structure 200." ('861 11:60-64) - "The output of the layout tool 300 may be a descriptive data structure 200 in the form of, for example, a text file. A secure packaging process 302a may accept container specific data as an input, and it may also accept the descriptive data structure 200 as a read only input. The packager 302a could be based on a graphical user interface and/or it could be automated. The packager 302a packages the container specific data 314 into a secure container 100." ('861 12:9-16) - "FIG. 24 shows an example of a user data element (UDE") 1200 provided by the preferred embodiment. As shown in FIG. 24, UDE 1200 in the preferred embodiment includes a public header 802, a private header 804, and a data area 1206. The layout for each of these user data elements 1200 is generally defined by an SGML data definition contained within DTD 1108 associated with one or more load modules 1100 that operate on the UDE 1200." ('193 143:21-28) - "The publisher 3308 may create or otherwise provide content and/or VDE control structure templates that are delivered to the local repository 3302 for use by other participants who have access to the "internal" network. The templates may be used to describe the structure of containers, and may further describe whom in the publisher 3308's organization may take which actions with respect to the content created within the organization related to publication for delivery to (and/or referencing by) the repository 3302. For example, the publisher 3308 may decide (and control by use of said temple) that a periodical publication will have a certain format with respect to the structure of its content and the types of information that may be included (e.g. text, graphics, multimedia presentations, advertisements, etc.), the relative location and/or order of presentation of its content, the length of certain segments, etc. Furthermore, the publisher 3308 may, for example, determine (through distribution of appropriate permissions) that the publication editor is the only party that may grant permissions to write into the container, and that the organization librarian is the only party that may index and/or abstract the content." ('193 294:65-295:18) - "templates may be represented as text files defining specific structures and/or component

Claim Term	MS Construction
	assemblies. Templates, with their structure and/or component assemblies may serve as VDE object authoring or object control applications. ('193 260:36-47) - "...The result of object definition 1240 may be an object configuration file 1240 specifying certain parameters relating to the object to be created. Such parameters may include, for example, map tables, key management specifications, and event method parameters. The object construction stage 1230 may take the object configuration file 1240 and the information or content to be included within the new object as input, construct an object based on these inputs, and store object repository 728." ('193 103:38-46) - "In accordance with one example, the machine readable descriptive data structure provides a description that reflects and/or defines corresponding structure(s) within the rights management data structure. For example, the descriptive data structure may provide a recursive, hierarchical list that reflects and/or defines a corresponding recursive, hierarchical structure within the rights management data structure. In other examples, the description(s) provided by the descriptive data structure may correspond to complex, multidimensional data structures having 2,3, or n dimensions. The descriptive data structure may directly and/or indirectly specify where, in an associated rights management data structure, corresponding defined data types may be found. The descriptive data structure may further provide metadata that describes one or more attributes of the corresponding rights management data and/or the processes used to create and/or use it. In one example , the entire descriptive data structure might be viewed as comprising such metadata." ('861 5:57- 6:7) - ('193 245:44-51); ('683 32:41-53); ('861 5:25-41); ('861 10:49-59); ('861 12:9-11); ('861 13:21-27); ('861 20:25-47); ('193 259:37-51); ('193 298:41-62); ('193 103:3-32); ('193 285:9-35); ('193 193:49-59); ('193 287:37-41) Extrinsic:
designating 721.1	Intrinsic: Extrinsic:
device class 721.1	Intrinsic: "Furthermore, Applicants respectfully submit that some of the terms cited by the Examiner as "indefinite" are either well-known by persons skilled in the art or inherently clear. For example, in Claims 1-4, 22-25, the term "class" is used as part of the phrase "device class." Applicants respectfully submit that "device class" is inherently clear, meaning a group of devices which share at least one attribute." (08/689,754 ('721), Amendment, 04/14/99, p. 14) Extrinsic: Device: 1. A mechanical, electrical, or electronic contrivance with a specific purpose.(IBM) Device class: The generic name for a group of device types.(IBM) Device type: 1. The name for a kind of device sharing the same model number; for example, 2311, 2400, 2400-1. Contrast with device class. (2) The generic name for a group of devices; for example, 5219 for IBM 5219 Printers. Contrast with device class. (IBM)
digital file 193.1, 193.11, 193.15, 193.19	Intrinsic: Extrinsic: File: "A complete, named collection of information, such as a program, a set of data used by a program, or a user-created document. A file is the basic unit of storage that enables a computer to distinguish one set of information from another. A file is the "glue" that binds a conglomeration of instructions, numbers, words, or images into a coherent unit that a user can retrieve, change, delete, save, or send to an output device." (Microsoft Computer Dictionary, 3rd ed., 1997)
digital signature, digitally signing	Intrinsic: - "There exist many well known processes for creating digital signatures. One example is the Digital

Claim Term	MS Construction
721.1	Signature Algorithm (DSA). DSA uses a public-key signature scheme that performs a pair of transformations to generate and verify a digital value called a "signature." ('721 10:60-64) - ('721 4:64-67); ('721 11:7-22); ('721 14:49-60); ('721 14:64-15:2) - "Certificates play an important role in the trustedness of digital signatures, and also are important in the public-key authentication communications protocol (to be discussed below). In the preferred embodiment, these certificates may include information about the trustedness/level of security of a particular VDE electronic appliance 600 (e.g., whether or not it has a hardware-based SPE 503 or is instead a less trusted software emulation type HPE 655) that can be used to avoid transmitting certain highly secure information to less trusted/secure VDE installations." ('193 203:58-67) Extrinsic: Digital Signature: In computer security, encrypted data, appended to or part of a message, that enables a recipient to prove the identity of the sender. (IBM) Digital Signature: 1. In authentication, data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery. 2. In authentication, a data block appended to a message, or a complete encrypted message, such that the recipient can authenticate the message contents and/or prove that it could only have originated with the purported sender. (Longley) "Let B be the recipient of a message M signed by A, then A' s [digital] signature must satisfy three requirements: 1. B must be able to validate A's signature on M. 2. It must be impossible for anyone, including B, to forge A's signature. 3. In case A should disavow signing a message M, it must be possible for a judge or third party to resolve a dispute arising between A and B. A digital signature therefore establishes sender authenticity [] it also establishes data authenticity." (Denning, p. 14)[7] "A cipher in unconditionally secure if, no matter how much ciphertext is intercepted, there is not enough information in the ciphertext to determine the plaintext uniquely." (Denning, p.5) (Davies, p. 41, 380) "A cipher is computationally secure, or strong, if it cannot be broken by systematic analysis with available resources." (Denning, p.5) (Davies, p.41, 370)
entity's control 891.1	Intrinsic: - "A public-key certificate is someone's public key "signed" by a trustworthy entity such as an authentic PPE 650 or a VDE administrator. " ('193 203:42-45) - "Distribution involves three types of entity. Creators usually are the source of distribution. The typically set the control structure "context" and can control the rights which are passed into a distribution network. Distributors are users who form a link between object (content) end users and object (content) creators. They can provide a two-way conduit for rights and audit data. Clearinghouses may provide independent financial services, such as credit and/or billing services, and can serve as distributors and/or creators. Through a permissions and budgeting process, these parties collectively can establish fine control over type and extent of rights usage and/or auditing activities." ('193 267:34-45) Extrinsic: Control: A business rule that governs the use of content. (ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply

[7] "Denning" herein refers to Denning, D., Cryptography and Data Security, 1983, MSI085569.

Claim Term	MS Construction
	to either a control program or a control set. (ITG, 1997-2000, ML00012D) Control: **Control Element*: A data structure that giverns (*sic)* the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). **Control mechanism*: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. **Control Parameter:* A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. (ITG, 3/7/95, IT00709618, see footnote 2) Control: Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node. (ITG, 5/12/95, IT00028293) Control: A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc. (ITG, 8/21/95, IT00032373, TD00068B)
environment 912.35, 900.155, 891.1, 683.2, 721.34	Intrinsic: '721 file history Rejection 10/15/98, Amendment 4/19/99 at 13-15 Extrinsic: "Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment.*" (ITG, 8/21/95, IT00032375, TD00068B)
executable programming, executable 912.8, 912.35, 721.34	Intrinsic: - "Furthermore, applicants' independent claims 16, 36, 37 and 64 require secure delivery and use of plural executable items. See claim 16 ("securely delivering a first procedure ... securely delivering ... a second procedure separable or separate from said first procedure..."); claim 36 ("securely delivering plural executable procedures ..."), claim 37 ("securely delivering a first piece of executable code ... securely delivering a second piece of executable code ...") and claim 64 ("securely receiving a first load module ... securely receiving a second load module ..."). These features are not taught or suggested by either Rosen or Johnson. Johnson's databases comprise data, not executable code." (08/388,107, Amendment, 06/20/97, p. 24-25) (MSI028848-49) "In addition, Applicants would like to draw the Examiner's attention to other sections of the specification in support of words or phrases cited by the Examiner as "indefinite." ... The noun "executable," as used in Claims ... 34-36 ..., is defined in the specification on page 7." (pg. 13-14) (page 7 of the original specification is '721 2:62-3:13 of the issued patent) (08/689,754 ('721), Amendment, 04/14/99, p. 14) Extrinsic: Execute: 1. To perform the actions specified by a program or a portion of a program.(IBM) Executable: 1. Program that has been link-edited and therefore can be run in a processor; The set of machine language instructions that constitute the output from the compilation of a source program.(IBM) Executable Programming: 1. A program that has been link-edited and therefore can be run in a processor. 2. The set of machine language instructions that constitute the output from the compilation of a source program.(IBM)
execution space, execution space	Intrinsic: - "One important security layer involves ensuring that certain component assemblies 690 are formed,

Claim Term	MS Construction
identifier 912.8	loaded and executed only in secure execution space such as provided within an SPU 500." ('193 87:35-38) - "The following is an example of a possible field layout for load module public header 802: ... Execution Space Code: Value that describes what execution space (e.g., SPE or HPE) this load module (sic)." ('193 140:15-35) - "The Ginter et al. patent disclosure describes, among other things, techniques for providing a secure, tamper resistant execution spaces within a "protected processing environment" for computer programs and data. The protected processing environment described in Ginter et al. may be hardware-based, software-based, or a hybrid. It can execute computer code the Ginter et al. disclosure refers to as "load modules."" ('721 3:16-23) "Furthermore, Applicants respectfully submit that some of the terms cited by the Examiner as "indefinite" are either well-known by persons skilled in the art or inherently clear. ... Furthermore, Applicants respectfully submit that the term "execution spaces," as used in Claim 32, is well-known in the art. It refers to a resource which can be used for execution of a program or process." 08/689,754 ('721), Amendment, 04/14/99, p. 14 - ('193 86:39-47); ('193 88:38-43); ('193 104:39-44); ('193 140:37-50) - "The SPE (HPE) load module execution manager ("LMEM") 568 loads executables into the memory managed by memory manager 578 and executes them. LMEM 568 provides mechanisms for tracking load modules that are currently loaded inside the protected execution environment. LMEM 568 also provides access to basic load modules and code fragments stored within, and thus always available to, SPE 503. LMEM 568 may be called, for example, by load modules 1100 that want to execute other load modules." ('193 111:20-28) - "The internal ROM 532 and RAM 534 within SPU 500 provide a secure operating environment and execution space." ('193 69:33-35) - SPU 500 general purpose RAM 534 provides, among other things, secure execution space for secure processes. ('193 70:43-44) Extrinsic: Execution: The process of carrying out an instruction or instructions of a computer program by a computer.(IBM) Tanenbaum
governed item 683.2	Intrinsic: - See "Allow" - "If an image representation of a signature is stored on portable media or in a directory service, the image may be stored in an electronic container 302. Such a container 302 permits the owner of the signature to specify control information that governs how the signature image may be used." ('683 27:29-) - VDE control information which governs the use, and consequences of use, of VDE controlled content." ('193 288:5-12) - ('193 128:41-45) Extrinsic: Govern: To initiate the execution of controls. (ITG, 10/2/96, IT00035894, TD00189F) Governance: The act of applying controls. Governance is the fundamental activity of the InterTrust Commerce Architecture. (ITG, 11/17/96, IT00035867, TD00189J) Governed Element: An InterTrust Commerce Architecture object to which governance is applied. DigiBox containers, content, control sets, and control records are the primary examples of governed

Claim Term	MS Construction
	elements. (ITG, 11/17/96, IT00035867, TD00189J) Defined consistent (IT 35962)
Halting 900.155	Intrinsic: - "Dynamic Check of Association Between Appliance and PPE Instance: The executing operational materials 3472 may next compare an embedded electronic appliance signature SIG' against the electronic appliance signature SIG stored in the electronic appliance itself (FIG. 69K, decision block 3564). As discussed above, this technique may be used to help prevent operational materials 3472 from operating on any electronic appliance 600 other than the one it was initially installed on. PPE 650 may disable operation if this machine signature check fails ("no" exit to decision block 3564, FIG. 69K; disable block 3566)." ('900 243:30-41) "When an inconsistency is detected ("yes" exit to decision block 3590, FIG. 69L), PPE 650 can take appropriate action such as locking itself up from further use until reconstructed under the trusted server's control (FIG. 69L, disable block 3591)." ('900 247:50-54) Extrinsic: Halt Indicators: In RPG, an indicator that stops the program when an unacceptable condition occurs. Valid halt indicators are H1-H9 (IBM) Halt Instruction: 1. A machine instruction that stops execution of a program. 2. Synonym for pause instruction. .(IBM)
host processing environment 900.155	Intrinsic: - ('193 63:13-17); ('193 79:60-67); ('193 81:4-8); ('900 230:57-61); ('900 231:23-31); ('900 236:505-53) - "HPE(s) 655 and SPE(s) 503 are self-contained computing and processing environments that may include their own operating system kernel 688 including code and data processing resources." ('193 79:36-39) - "HPEs 655 may be provided in two types: secure and not secure." ('193 80:8-9) - ('193 79:31); ('193 80:22-36); ('193 80:40-65, Fig. 10); ('193 88:31-43); ('193 104:39-44) Extrinsic: Host processor : 1. A processor that controls all or part of a user application network. 2. In a network, the processing unit in which resides the access method for the network. 4. A processing unit that executes the access method for attached communication controllers.(IBM) "Host Processing Environment (HPE): A software-only realization of the PPE, protected from tampering by appropriate software techniques. No longer preferred because of the potential confusion between the "H" in the acronym and "H" as in "Hardware" (which this isn't). [REPLACEMENT UNCERTAIN]" (ITG, 3/7/95, IT00709621)[8] "Secure Processing Environment (SPE): A hardware-supported realization of the PPE, protected from tampering by physical security techniques. No longer preferred because of the potential confusion between the "S" in the acronym and "S" as in "Software" (which this isn't). [REPLACEMENT UNCERTAIN]" (ITG, 5/12/95, IT00028302) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*. (ITG, 8/21/95, IT00032375, TD00068B)
identifier, identify,	Intrinsic:

[8] Obsolete Terminology Section: "This section identifies terms that have been used in earlier documents to describe various VDE concepts, but that are, for various reasons, no longer preferred."

Claim Term	MS Construction
identifying 193.11, 193.15, 912.8, 912.35, 861.58	- "Portable appliance 2600 RAM 534 may contain, for example, information which can be used to uniquely identify each instance of the portable appliance. This information may be employed (e.g. as at least a portion of key or password information) in authentication, verification, decryption, and/or encryption processes." ('193 230:22-27) - ('193 25:31-38); ('193 37:27-31); ('193 111:47-67) ('193 111:59-67); ('193 124:8-18); ('193 131:40-45); ('193 139:41-55); ('193 214:39-41) ('861 12:63-13:4); ('193 67:21-26); ('193 209:63-67); ('193 214:39-41) Extrinsic: Identifier: 1. One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element. 2. In programming languages, a token that names a data object such as a variable, an array, a record, a subprogram or a function. (IBM) Identifier: 1. In computing, a character or group of characters used to identify, indicate or name a body of data. 2. In computing, a name or string of characters employed to identify a variable, procedure, data structure or some other element of a program. (Longley)
including 193.1 (at 320:63, and 321:3); 193.19 (at 324:15); 912.8 (at 327:36, 39, and 41); 912.35 (330:35 and 39); 861.58 (at 26:53 and 63); and 683.2 (at 63:60).	Intrinsic: - Prosecution History of '900 Patent: Changed "including" to "comprising" "to avoid any possible ambiguity relating to whether the control information must be 'inside' the secure object." Amendment to allowed claim 60, 10/29/98. - "Load modules 1100 in the preferred embodiment comprise executable code, and may also include or reference one or more data structures called "data descriptor" ("DTD") information." ('193 136:53-56) - "include or reference" ('861 15:21) - "including or addressing" (claim 58); - "includes a reference to" (claim 69); - "Secure database 610 in the preferred embodiment does not include VDE objects 300, but rather references VDE objects stored, for example, on file system 687 and/or in a separate object repository 728." ('193 126:26-65) - ('193 131:18-20) Extrinsic: "3. To consider with or place into a group, class, or total: thanked the host for including us." (Amer. Heritage Dictionary, 4th ed.)
information previously stored 900.155	Intrinsic: Extrinsic: Information: 1. In information processing, knowledge concerning such things as facts, concepts, objects, events, ideas, and processes, that within a certain context has a particular meaning. (IBM) Information: 1. Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape. 3. Knowledge that was unknown to the receiver prior to its receipt. Information can only be derived from data that is accurate, timely, relevant and unexpected.(Longley) Store: 1. To place data into a storage device. 2. To retain data in a storage device.

Claim Term	MS Construction
integrity programming 900.155	Intrinsic: - "Upon initialization, the operational materials 3472 validate the embedded signature value against the actual electronic appliance 600 signature SIG, and may refuse to start if the comparison fails." ('900 239:21-25)[i] - "an otherwise unused section of the non- volatile CMOS RAM 656a may be used to store a signature 3497d. Signature 3497d is verified against the PPE 650's internal state whenever the PPE is initialized." ('900 239:51-55) - "Dynamic Check of Association Between Appliance and PPE Instance: The executing operational materials 3472 may next compare an embedded electronic appliance signature SIG' against the electronic appliance signature SIG stored in the electronic appliance itself (FIG. 69K, decision block 3564). As discussed above, this technique may be used to help prevent operational materials 3472 from operating on any electronic appliance 600 other than the one it was initially installed on. PPE 650 may disable operation if this machine signature check fails ("no" exit to decision block 3564, FIG. 69K; disable block 3566)." ('900 243:30-41) - ('193 80:45-48) Extrinsic: Integrity: The protection of systems, programs, and data from inadvertent or malicious destruction or alteration.(IBM) Integrity: 1. In data security, that computer security characteristic that ensures that computer resources operate correctly and that the data in the databases are correct. 2a. In data security, the capability of an automated system to perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. 2b. In data security, inherent quality of protection that ensures and maintains the security of entities of a computer system under all conditions.(Longley) Programming: 1. A sequence of instructions suitable for processing by a computer. 2. In programming languages, a logical assembly of one or more interrelated modules. 4. A sequence of instructions that a computer can interpret and execute.(IBM) Programming: The process by which a computer is made to perform a specialized task. It involves the creation of a formalized sequence of instructions which can be recognized and implemented by the machine. (Longley) Integrity: The ability to verify that data is unmodified from its intended value. (ITG, 5/12/95, IT00028294) Integrity: In relation to digital content, a state in which that content is unmodified and operations on the content are performed only as specified by the rightsholders. DigiBox containers ensure integrity. (ITG, 10/2/96, IT00035895, TD00189F) Integrity: definition varies slightly, best seems to be – A state in which content is unmodified and operations on properties are performed only as specified by the rights holders (IT 35922). Integrity: The assurance that content in a DigiBox container or content being processed by an IT content node has not been tampered with. (IT 35868)
key 193.19	Intrinsic: "Key Types The detailed descriptions of key types below further explain secret-key embodiments; this summary is not intended as a complete description. The preferred embodiment PPE 650 can use different types of keys and/or different "shared secrets" for different purposes. Some key types apply to a Public-Key/Secret Key implementation, other keys apply to a Secret Key only implementation, and still other key types apply to both. The following table lists examples of various key and "shared secret"

Claim Term	MS Construction
	information used in the preferred embodiment, and where this information is used and stored: Key/Secret Information Type — Used in PK or Non-PK — Example Storage Location(s) Master Key(s) (may include some of the specific keys mentioned below) — Both — PPE Manufacturing Key — Both (PK optional) — Manufacturing facility Certification key pair — PK — VDE administrator Public/private key pair — PK — PPE (PK case) Initial secret key — Non-PK — Manufacturing facility PPE manufacturing ID — Non-PK — PPE Site ID, shared code, shared keys and shared secrets — Both — Certification repository Download authorization key — Both — PPE External communication keys and other info — Both — Certification repository (Public Key only) Administrative object keys — Both — PPE Stationary object keys — Both — PPE Traveling object shared keys — Both — PPE Secure database keys — Both — Secure Database Private body keys — Both — Permission record Content keys — Both — Permission record Authorization shared secrets — Both — PPE Secure Database Back up keys — Both — Secure database" ('193 211:32 – 212:11) - ('193 211:18-212:18); ('193 193:8-23); ('193 207:50-60); ('193 208:38-40) Extrinsic: Keys: The permissions record also contains the fundamental decryption keys for an object. It may contain the keys for the object content or keys to decrypt portions of the object that contain other keys that then can be used to decrypt the content of the object. Usage of the keys is controlled by the Control Sets in the same permissions record. There are many more aspects to the keys in the permissions record that are beyond the scope of this document. (VDE ROI DEVICE v1.0a 9 Feb 1994, IT00008601) Key: 7. In computer security, a sequence of symbols used with a cryptographic algorithm for encrypting or decrypting data. (IBM) Key: 1. In cryptography, a sequence of symbols that controls the operations of encipherment and decipherment. 2. In cryptography, a symbol or sequence of symbols (or electrical or mechanical correlates of symbols) that control the operations of encryption and decryption). (Longley)
load module 912.8, 721.1	Intrinsic: Prosecution History of Application 08/388,107 ('912 Patent is continuation) "Furthermore, applicants' independent claims 16, 36, 37 and 64 require secure delivery and use of plural executable items. See claim 16 ("securely delivering a first procedure ... securely delivering ... a second procedure separable or separate from said first procedure..."); claim 36 ("securely delivering plural executable procedures ..."), claim 37 ("securely delivering a first piece of executable code ... securely delivering a second piece of executable code ...") and claim 64 ("securely receiving a first

Claim Term	MS Construction
	load module ... securely receiving a second load module ..."). These features are not taught or suggested by either Rosen or Johnson. Johnson's databases comprise data, not executable code." 08/388,107, Amendment, 06/20/97, p. 24-25 (MSI028848-49) - "Load module 1100 contains code and static data (that is functionally the equivalent of code), and is used to perform the basic operations of VDE 100. Load modules 1100 will generally be shared by all the control structures for all objects in the system, though proprietary load modules are also permitted. Load modules 1100 may be passed between VDE participants in administrative object structures 870, and are usually stored in secure database 610. They are always encrypted and authenticated in both of these cases. When a method core 1000' references a load module 1100, a load module is loaded into the SPE 503, decrypted, and then either passed to the electronic appliance microprocessor for executing in an HPE 655 (if that is where it executes), or kept in the SPE (if that is where it executes)." ('193 139:19-32) - ('193 20:27-30); ('193 71:19-40); ('193 77:12-29) ('193 86:49-60); ('193 87:41-62); ('193 109:24-45); ('193 111:20-28); ('193 111:29-39); ('193 111:40-47); ('193 111:59-67); ('193 126:30); (193 139:28-31); ('193 139:60-140:6); ('193 140:1-6); ('193 140:44-50); ('193 141:42-55); ('193 209:52-210:35); ('193 17:15-17); ('193 20:27-30); ('193 86:39-48); ('193 139:41-51); ('193 151:20-22); ('721 3:21-35) Extrinsic: Load module: 1. All or part of a computer program or subprogram in a form suitable for loading into main storage for execution by a computer; usually the output of a linkage editor.(IBM) Load Module: A procedure, dynamically loaded or resident within the PPE, that performs or controls operations within the PPE. Some load modules are associated with individual objects or types of objects; others perform general utility operations. (ITG, 3/7/95, IT00709618 see footnote 2) "Load Module: shall mean an executable program that, when combined with control data and/or parameters, forms procedures or programs for performing specific types of control functions in compliance with EPR Specifications. Load Modules and their executable programs and associated control data and/or parameters are designed to, at least in part, be employed as one or more control elements which are used within a protected information transaction/distribution management arrangement." (License Agreement between National Semiconductor and EPR, 3/18/94, Exhibit 12 to InterTrust 30(b)(6)) "Load Module: The lowest level of a VDE control structure: an executable program that operates, under control of a *method* or another *load module,* to manipulate VDE-protected elements (which may be in *containers* otherwise)." (IT VDE Container Overview, 2/10/95, IT00051228, ETM-9999 Version 0.21) "A load module is an executable program that manipulates VDE elements and content to perform a specific control function. A load module invoked as an external method is responsible for ensuring that all its related load modules, methods, elements, etc. are available and that all required option choices have been made." (IT VDE Container Overview, 2/10/95, IT00051234, ETM-9999 Version 0.21)
Machine check programming 900.155	Intrinsic: - "machine check" does not appear in specification - "Correspondence Between Installed Software and Appliance "Signature". Another technique that may be used during the installation routine 3470 is to customize the operational materials 3472 by embedding a "machine signature" into the operational materials to establish a correspondence between the installed software on a particular electronic appliance 600 (FIG. 69C, block 3470(7)). ('900 239:4-14) - For electronic appliances 600 where it is feasible to do so, the installation procedure 3470 may determine unique information about the electronic appliance 600 (e.g., a "signature" SIG in the sense of a unique value—not necessarily a "digital signature" in the cryptographic sense)." ('900 239:15-19)

Claim Term	MS Construction
	- "FIG. 69G shows an example of some of these appliance-specific signatures." ('900 239:41-42) - "Dynamic Check of Association Between Appliance and PPE Instance: The executing operational materials 3472 may next compare an embedded electronic appliance signature SIG' against the electronic appliance signature SIG stored in the electronic appliance itself (FIG. 69K, decision block 3564). As discussed above, this technique may be used to help prevent operational materials 3472 from operating on any electronic appliance 600 other than the one it was initially installed on. PPE 650 may disable operation if this machine signature check fails ("no" exit to decision block 3564, FIG. 69K; disable block 3566)." ('193 243:30-) - "Signature 3497d may also be updated whenever a significant change is made to the secure database 610. If the CMOS RAM signature 3497d does not match the database value, PPE 650 may take this mismatch as an indication that a previous instance of the secure database 610 and/or PPE 650 software has been restored, and appropriate action can be taken. ('900 239:55-240:6) - ('900 240:15-26); (900 Claim 183) Extrinsic: Machine check: An error condition that is caused by an equipment malfunction. (IBM)
Metadata information 861.58	Intrinsic: - "This metadata can define certain characteristics associated with the object name. For example, such metadata may impose integrity or other constraints during the creation and/or usage process (e.g., "when you create an object, you must provide this information", or "when you display the object, you must display this information"). The metadata 264 may also further describe or otherwise qualify the associated object name." ('861 15:21-31) - (861 Abstract); ('861 6:2-7); ('861 8:57-64); ('861 13:30-34); ('861 14:7-11); ('861 16:37-52) Extrinsic: Metadata: In databases, data that describe data objects. (IBM) Information: 1. In information processing, knowledge concerning such things as facts, concepts, objects, events, ideas, and processes, that within a certain context has a particular meaning.(IBM) Metadata: 1. In computing, data referring to other data (such as data structures, indices, and pointers) that are used to instantiate an abstraction (such as 'process,' 'task,' 'segment,' 'file,' or 'pipe') 2. In computing, a special database, also referred to as a data dictionary, containing descriptions of the elements. (Longley)
opening secure containers 683.2	Intrinsic: - "Because container 152 can only be opened within a secure protected processing environment 154 that is part of the virtual distribution environment described in the above-referenced Ginter et al. patent disclosure" ('712 168:22-25) - Special mathematical techniques known as "cryptography" can be used to make electronic container 302 secure so that only intended recipient 4056 can open the container and access the electronic document (or other item) 4054 it contains. ('683 15:67-16:4) - The appliance 600 may then open the secure electronic container ("attaché case") 302 and deliver the item it contains to recipient 4056 (FIG. 91B, block 4092D). ('683) - Appliance 600 may then generate a "send" or "open" event to PPE 650 requesting the PPE to open container 302 and allow the user to access its contents. - ('193 185:7-30); ('193 185:42-46); ('683 19:27-32); ('193 183:28-29); ('193 183:55-57); ('193 185:11-16) Extrinsic: Open: 1. The function that connects a file to a program for processing. 4. To prepare a file for

Claim Term	MS Construction
	processing. (IBM) Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Container: In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers. (Longley) Container: contains protected content which is divided into one or more atomic elements, and optionally, PERCs governing the content and may be manipulated only as specified by a PERC. (ITG, 3/7/1995, IT00709616) Container: A protected (encrypted) storage object that incorporates descriptive information, protected content, and (optionally) control objects applicable to that content. (ITG, 3/7/1995, IT00709617, see footnote 3) Container: A protected digital information storage and transport mechanism for packaging content and control information. (ITG, 8/21/95, IT00032372, TD00068B]
operating environment 891.1	Intrinsic: Extrinsic: Operating Environment: The physical environment; for example, temperature, humidity, and layout.(IBM) Operating system: In computing, a collection of software programs intended to directly control the hardware of a computer and on which all the other programs running on the computer generally depend.(Longley) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*. (ITG, 8/21/95, IT00032375, TD00068B) Operation: A manipulation of some protected resource (e.g., content in a *container* or control records in a *PERC*) (IT VDE Container Overview, 2/10/95, IT00051228, ETM-9999 Version 0.21)
organization, organization information, organize 861.58	Intrinsic: - "a descriptive data structure could serve as `instructions` that drive an automated packaging application for digital content and/or an automated reader of digital content such as display priorities and organization (e.g., order and/or layout)."('861 7:54-57); - For example, the descriptive data structure may provide a recursive, hierarchical list that reflects and/or defines a corresponding recursive, hierarchical structure within the rights management data structure ('861 5:57-63)". ... descriptive data structure may directly and/or indirectly specify where, in an associated rights management data structure, corresponding defined data types may be found." ('861 5:67-6:2); - Issued claim 1: a first memory storing a descriptive data structure, said descriptive data structure including: information regarding a first organization of elements within a secure container, said information including: information on the organization of said elements within said secure container; and information on the location of at least some of said elements within said secure container" - Issued claim 34: "a representation of the format of data contained in a first rights management data structure said representation including: element information contained within said first rights management data structure; and organization information regarding the organization of said elements within said first rights management data structure; and information relating to metadata, said metadata including" - Issued claim 45 (dependent from 34-44): "said information regarding elements contained within said first rights management data structure includes information relating to the location of at least one such element." - Issued claim 73: "said descriptive data structure organization information includes information

Claim Term	MS Construction
	specifying that said first secure container contents will include at least a title and a text section referred to by said title." - Issued claim 74: "said descriptive data structure organization information includes information specifying that said first secure container contents will include at least one advertisement." - Issued claim 75: "said descriptive data structure further includes information relating to the location at which said title, said text section and said advertisement should be stored in said first secure container." - Issued claim 76: "at least a portion of said descriptive data structure organization information includes information specifying fields relating to at least one atomic transaction" ('193 103:23-46) Extrinsic:
portion 193.1, 193.11, 193.15, 193.19, 912.8, 912.35, 861.58	Intrinsic: Extrinsic: Portion: "1. A section or quantity within a larger thing; a part of a whole. 2. A part separated from a whole." (American Heritage Dictionary 4th Ed.)
prevents 721.34	Intrinsic: - "VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:51-56) - "VDE ensures that certain prerequisites necessary for a given transaction to occur are met." ('193 20:27-28) - "For example, shrink-wrapping does not prevent the constant illegal pirating of software once removed from either its physical or electronic package." ('193 5:60-62) "VDE, for example, provides the ability to prevent, or impede, interference with and/or observation of, important rights related transactions and processes. VDE, in its preferred embodiment" ('193 4:1-4) "After receiving enabling distribution control information from creator A, distributor A may manipulate an application program to specify some or all of the particulars of usage control information for users and/or user/distributors enabled by distributor A (as allowed, or not prevented, by senior control information)." ('193 303:63) - ('193 6:33-35); ('193 15:41-46); ('193 17:22-28); ('193 309:10-16); ('193 303:63-304:1) Extrinsic:
processing environment 912:35, 900:155, 721:34, 683.2	Intrinsic: - "Another approach to supporting COTS software would use the VDE software running on the user's electronic appliance to create one or more "virtual machine" environments in which COTS operating system and application programs may run, but from which no information may be permanently stored or otherwise transmitted except under control of VDE." ('193 279:26-40) - "VDE may be combined with, or integrated into, many separate computers and/or other electronic appliances. These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc. The secure subsystem in the preferred embodiment comprises one or more "protected processing environments", ..." ('193 9:22) - ('193 9:22-29); ('683 24:26-33); ('193 60:51-64)

Claim Term	MS Construction
	Extrinsic: Processing: 1. The performance of logical operations and calculations on datum including temporary retention of data in processor storage while the data is being operated on.(IBM) Process: (1) in computing, the active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. 2. In computing, a program in execution. ... (4) In computing, a program is a static piece of code and a process is the execution of that code. (Longley) Environment: 1. The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. 2. In computer security, those factors, both internal and external, of an ADP system that help to define the risks associated with its operation (Longley) Secure Processing Environment (SPE): A hardware-supported realization of the PPE, protected from tampering by physical security techniques. No longer preferred because of the potential confusion between the "S" in the acronym and "S" as in "Software" (which this isn't). [REPLACEMENT UNCERTAIN] (ITG, 5/12/95, IT00028302) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*. (ITG, 8/21/95, IT00032375, TD00068B)
protected processing environment 721:34, 683.2	See also "secure" Intrinsic: Prosecution History of Application 08/778,256 (continuation of '891 Patent, issued at USP 5,949,876) "Independent claims 65 and 76 each recite a "protected processing environment." ... Griffeth et al. [U.S. Pat. No. 5,505,837], Yamamoto [U.S. Pat. No. 5,508,913] and Wyman [U.S. Pat. No. 5,260,999] do not disclose these aspects of these claims. The system disclosed in Griffeth et al is designed to allow negotiation to proceed in an environment in which a negotiating party does not disclose information about its negotiation goals to the other negotiating party. ... Griffeth et al. does not disclose any privacy protection mechanism and neither teaches nor suggests any secure processing environment or that any operations (e.g., integration or execution) occur securely. Indeed, Griffeth contains no suggestion that any protection mechanism is needed to maintain negotiation goals in privacy, since Griffeth does not suggest that the other party may try to improperly discover information which is intended to remain private. Yamamoto states the following: "Here, the data is enciphered by the data encipher apparatuses 26 so as to maintain confidentiality." Col. 3, lines 46-47. Since Yamamoto makes no other reference to the encipherment, or to the apparatuses 26, it is impossible to determine how the data encipherment is used, or the roles it plays in the disclosed apparatus. From an examination of Fig. 3, however, it appears that the data encipher apparatuses 26 are placed on connections between a particular site and other, physically separated sites. For example, customer office 23b is connected to sub-center 22 by a line, which apparently represents a communication path. That line connects directly to a data encipher apparatus 26 in customer office 23b, and to another data encipher apparatus 26 in sub-center 22. Thus, it appears that the data encipher apparatuses 26 are used, in some undisclosed manner, to encipher at least some data which travels among physically separated locations. It is possible to imagine, for example, that data is enciphered prior to being sent out on an insecure public transmission line, and is then deciphered once received in a new location. Yamamoto does not disclose, however, that the processing environments are themselves secure, or that either execution or integration occur in a secure manner or in a secure environment. Indeed, Yamamoto contains no suggestion that security within a processing environment would even be desirable. By suggesting that data is deciphered once it enters an office (e.g., office 23b), in fact, Yamamoto teaches away from a secure environment, since it would appear that the data is used "in the clear" within the office, with no suggested protection beyond a simple password for the computer.

Claim Term	MS Construction
	Wyman is equally deficient regarding these elements. Although Wyman specifies that a license may contain a digital signature, therefore rendering the license unforgeable (Col. 14, lines 24-54), Wyman neither teaches nor suggests that the processing environment is itself secure or that any operations occur in a secure manner. The Wyman digital signatures no more suggest a secure processing environment than the requirement that paper contracts be signed in ink suggests that the contracts will be created, read or negotiated in a secure location." 08/778,256 ('876), Amendment, 01/20/98, p. 58-60 - "The role of go-between 4700 may, in some circumstances, be played by one of the participant's SPU's 500 (PPEs), since SPU (PPE) behavior is not under the user's control, but rather can be under the control of rules and controls provided by one or more other parties other than the user (although in many instances the user can contribute his or her own controls to operate in combination with controls contributed by other parties)." ('683 24:26) - "SPU 500 provides a tamper-resistant protected processing environment ("PPE") in which processes and transactions can take place securely and in a trusted fashion." ('683 16:60-62) - "The computer 3372 may then execute the operational materials 3472 from its hard disk 3376 to provide software-based protected processing environment 650 and associated software-based tamper resistant barrier 672) ('900 231:27-31)); - ('193 20:58-63); ('193 21:11-17); ('721 7:19-23); ('721 16:64-17:5); - "HPE(s) 655 and SPE(s) 503 are self-contained computing and processing environments that may include their own operating system kernel 688 including code and data processing resources." ('193 79:36-39) - (see Figs. 10 and 13), ('193 79:24), (105:23, 105:43, 109:46); ('193 13:7-23); ('193 223:30-44) - "In one example, a person with a laptop 5102 or other computer lacking a PPE 650 wishes nonetheless to take advantage of a subset of secure item delivery services." ('683 62:17-20) "Claims 7-11, ... 99-111 ... are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (5,412,717) in view of Narasimhalu et al (5,499,298). Fischer discloses a method and apparatus including a system monitor which limits the ability of a program about to be executed to the use of predefined resources, ... The set of authorities and restrictions are referred to as "program authorization information" or "PAI". ... A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... memory containing a first rule corresponds to a first PAI under a first PCB ... ... Here, Fischer provides a secure container in the form of a program, i.e. a governed item, having an associated PAI, i.e. at least one rule associated with the secure container. A protected processing environment ("PPE") protecting at least some information contained in the PPE, see Fischer Terminal A, and including hardware and/or software used for applying said first rule and the secure container in combination to at least in part govern at least one aspect of access to or use of the governed item, see Fischer at Figure 5 and column 10, lines 8-39 where the first rule in memory is first PCB providing a first PAI and the secure container is a program associated with a second PCB providing a first PAI and the secure container is a program associated with a second PCB having a second PAI associated with the governed item, i.e. the program. ... The difference between claim 7 and Fischer is that the PPE disclosed in Fischer is not explicitly disclosed as protected from tampering by a user of the first apparatus, i.e. terminal A. The Narasimhalu patent (hereinafter '298) teaches a method and apparatus for controlling the dissimenation of digital information. [and] that the end user accesses the digital information with a tamper-proof controlled information access device." 09/221,479 ('683), Office Action, 11/12/99, p. 3-5 (IT00065799-801) "With respect to the remaining issues, Applicants respectfully disagree. For example, the Examiner objects to the use of "environment" as indefinite and unclear. This word, however, is not used in isolation, but rather in the context of several longer phrases, all of which are defined in the specification. The phrase "protected processing environment," for example, is used in Claims 11 and 15-18 and described on at least, for example, pages 7-8 and 25 of the specification. The term "virtual

Claim Term	MS Construction
	distribution environment" used in Claim 11 is described, for example, on page 7 of the specification. The terms are also described in the commonly copending application Serial Number 08/388,107 of Ginter et al., filed 13 February 1995, entitled "System and Methods for Secure Transaction Management and Electronic Rights Protection." A copy of the incorporated Ginter application can be provided to the Examiner upon request." (pages 7, 7-8 and 25 of the original specification are '721 2:62-3:13, 2:62-3:34 and 8:6-28 of the issued patent) "The role of go-between 4700 may, in some circumstances, be played by one of the participant's SPU's 500 (PPEs), since SPU (PPE) behavior is not under the user's control, but rather can be under the control of rules and controls provided by one or more other parties other than the user (although in many instances the user can contribute his or her own controls to operate in combination with controls contributed by other parties)." ('683 24:26) 08/689,754 ('721), Amendment, 04/14/99, p. 13 Extrinsic: Processing: 1. The performance of logical operations and calculations on datum including temporary retention of data in processor storage while the data is being operated on.(IBM) Environment: 1. The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. 2. In computer security, those factors, both internal and external, of an ADP system that help to define the risks associated with its operation (Longley) - IT used "tm" symbol with "Protected Processing Environment" (Panel Abstract: The InterTrust Commerce Architecture, presented at 20th NISSC, 1997) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment.* (ITG, 8/21/95, IT00032375, TD00068B) Protected Processing Environment (PPE) technology: The InterTrust technology that provides the protected software environment within the InterRights Point. Protected Processing Environment technology is responsible for the encryption/decryption of data, protected processing of DigiBox containers, and other secure operations, such as protected database access. (ITG, 1997-1998, ML00012B) Protected Processing Environment (PPE): The PPE is the secure part of a VDE node: either a hardware or software-protected environment in which VDE mechanisms run without external interference. There are various PPE realizations (e.g., physically protected hardware) appropriate to different operational requirements (ITG, 3/7/1995, IT00709619, see footnote 2) Secure Processing Unit: The physically secure hardware component of the SPE: a processor with local memory and non-volatile storage. The SPE consists of the SPU itself and the SPE software running on the SPU. (ITG, 3/7/1995, IT00709620, see footnote 2) "Protected Processing Environment (PPE): An InterTrust *node* has a unique *node ID* and contains a *Protected Processing Environment (PPE)* which performs *operations* on *containers* and *control structures* under rules specified by *PERCs* and which may be realized in a tamper resistant hardware component or in tamper-resistant software and a *protected database*, which stores *control objects* and *InterTrust applications*, operating outside the *PPE*, which manipulate *content* and *control objects* through requests to the *PPE*" (ITG, 4/06/95, IT00028206) "All the terms in italics have specific definitions (in the glossary) with respect to InterTrust." 950406: *Global replace of "VDE" with "InterTrust" to match new terminology.* (ITG, 4/06/95, IT00028206) Protected Environment: A portion of the node software that uses, and protects, the protected node data

Claim Term	MS Construction
	such as cryptographic keys. The protected environment is responsible for performing all the protected functions for manipulating containers and content; that is, all the operations governed by controls. (ITG, 5/12/95, IT00028294) Protected Processing Environment: (alternate definition): The protected environment in which the cryptographic and control functions of InterTrust run. The PPE may be protected environmentally (e.g., as a physically protected server machine) or may employ software-based tamper resistance techniques. (ITG, 8/21/95, IT00032377, TD00068B) Secure Processing Environment (SPE): A hardware-supported realization of the PPE, protected from tampering by physical security techniques. No longer preferred because of the potential confusion between the "S" in the acronym and "S" as in "Software" (which this isn't). [REPLACEMENT UNCERTAIN] (ITG, 5/12/95, IT00028302) Protected Processing Environment (PPE): The InterTrust protected software environment within the InterTrust Commerce Node. The PPE is responsible for the encryption/decryption of data, protected processing of DigiBox containers, and other secure operations, such as database access. (ITG, 11/17/96, IT00035871, TD00189J)
protecting 683.2	Intrinsic: - VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:51-56) - "An attacker would gain little benefit from intercepting this information since it is transmitted in protected form; she would have to compromise electronic appliance 600(1) or 600(N) (or the SPU 500(1), 500(N)) in order to access this information in unprotected form." ('193 228:25) - Even if the object is stored locally to the VDE node, it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ('193 192:14-17) - ('193 228:25-30); ('193 6:33-35); ('193 15:41-46); ('193 17:22-28) Extrinsic: Hoffman, Modern Methods for Computer Security & Privacy at 134 Dictionary of Computing, 3rd Ed. (1990) ("Protected Location: A memory location that can only be accessed by an authorized user or process."; "Protected domain: A set of access privileges to protected resources.") Webster's New World Dictionary of Computer Terms, 4th Ed. (1992) ("To prevent unauthorized access to programs or a computer system; to shield against harm.") The New IEEE Standard Dictionary of Electrical and Electronics Terms, 5th Ed. (1993) ("Protection: (1) (computing systems). See: Storage protection (2) (software). An arrangement for restricting access to or use of a all, or part, of a computer system." ; "Storage protection: An arrangement for preventing access to storage for either reading or writing, or both.") IN00862862 Security: The combination of integrity and secrecy, applied to data. (ITG, 5/12/95, IT00028295) Secrecy: The inability to obtain any information from data. (ITG, 5/12/95, IT00028294)
record (n.) 912.8, 912.35	Intrinsic: "The selected method event record 1012, in turn, specifies the appropriate information (e.g., load module(s) 1100, data element UDE(s) and MDE(s) 1200, 1202, and/or PERC(s) 808) used to construct

Claim Term	MS Construction
	a component assembly 690 for execution in response to the event that has occurred. ..." ('193 138:12-47) Extrinsic: Record: 1. In programming languages, an aggregate that consists of data objects, possibly with different attributes, that usually have identifiers attached to them. In some programming languages, records are call structures. 2. A set of data treated as a unit. 3. A set of one or more related data items grouped for processing. (IBM) Record: 1. In computing, a collection of related data treated as a unit, e.g. details of name, address, age, occupation and department of an employee in a personnel file. 2.. In computing, to store signals on a recording medium for later use. (Longley) New IEEE Standard Dictionary of Electrical and Electronics Terms (5th ed. 1993)
required 912.8, 861.58	Intrinsic: See "allow." Extrinsic:
resource processed 891.1	Intrinsic: - ('193 72:39-44); ('193 75:15-30); ('193 283:23-28) "Smart objects may have the means to request use of one or more services and/or resources. Services include locating other services and/or resources such as information resources, language or format translation, processing, credit (or additional credit) authorization, etc. Resources include reference databases, networks, high powered or specialized computing resources (the smart object may carry information to another computer to be efficiently processed and then return the information to the sending VDE installation), remote object repositories, etc. Smart objects can make efficient use of remote resources (e.g. centralized databases, super computers, etc.) while providing a secure means for charging users based on information and/or resources actually used." ('193 38:60-39:8) Extrinsic: Resource: 1. Any of the data processing system elements needed to perform required operations, including storage, input/output units, one or more processing units, data, files, and programs. 2. Any facility of a computing system or operating system required by a job or task, and including main storage, input/output devices, processing unit, data sets, and control or processing programs.(IBM) Processed: 1. The performance of logical operations and calculations on datum including temporary retention of data in processor storage while the data is being operated on. (IBM) Process: (1) in computing, the active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. 2. In computing, a program in execution. (4) In computing, a program is a static piece of code and a process is the execution of that code. (Longley)
rule 861.58, 683.2	Intrinsic: - "A system as in claim 17, said memory further storing at least one rule associated with said first secure container, said first secure container rule at least in part governing at least one aspect of access to or use of said governed item. A system as in claim 19, said at least first secure container rule further including a second rule at least

Claim Term	MS Construction
	in part restricting the number of accesses and/or uses a user may make of said governed item." 09/221,479('683), Preliminary Amendment, 12/28/99, p. 5 (IT00065690) "Claims 7-11, ... are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (5,412,717) in view of Narasimhalu et al (5,499,298). Fischer discloses a method and apparatus including a system monitor which limits the ability of a program about to be executed to the use of predefined resources, ... The set of authorities and restrictions are referred to as "program authorization information" or "PAI". ... A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... memory containing a first rule corresponds to a first PAI under a first PCB ... ... Here, Fischer provides a secure container in the form of a program, i.e. a governed item, having an associated PAI, i.e. at least one rule associated with the secure container." 09/221,479 ('683), Office Action, 11/12/99, p. 3-4 (IT00065799-800) - In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed.. ('193 6:24-30) - "at least one rule and/or control associated with the software agent that governs the agent's operation." ('193 241:2-3) - "FIG. 4 illustrates examples of some different types of rules and/or control information" ('683 11:37-38) - "If necessary, trusted go-between 4700 may obtain and register any methods, rules and/or controls it needs to use or manipulate the object 300 and/or its contents (FIG. 122 block 4778)." ('683 47:40-45) - "In this further user interaction provided by object submittal manager 774, the user may specify permissions, rules and/or control information to be applied to or associated with the new object 300." ('193 106:60) - "at least one rule and/or control associated with the software agent that governs the agent's operation." ('193 241:2) - "The usage-related "rules and controls" may, for example, specify what a user can and can't do with the content and how much it costs to use the content." ('193 55:46-49) - "Container 300x is specified as a content object that is empty of content. It contains a control set that contains the following rules: 1. A write_without_billing event that specifies a meter and a general budget that limits the value of writing to $15.00. 2. Audits of usage are required and will be stored in object 300w under control information specified in that object. 3. An empty use control set that may be filled in by the owner of the information using predefined methods (method options)." ('193 243:35-37) - "an object creator or other provider can specify within a descriptive data structure 200, certain rules, integrity constraints and/or other characteristics that can or should be applied to the object after it has been imported into a target rights management environment." ('861 17:49-53) - ('683 54:29-37); ('193 56:28-35); ('193 53:60-63); ('683 47:40-45) Extrinsic: Rule: In computing, a statement in an expert system that enables the likelihood of an assertion, or the value of an object, to be established. A rule combines lower level assertions or objects to produce a value for a higher level assertion or object. (Longley) See Business Rule: A specification of the conditions governing how content and controls in DigiBox containers may be manipulated. A business rule may specify pricing, terms of use terms, operational

Claim Term	MS Construction
	restrictions, payment methods, and other aspects of information use. A rule may also specify consequences related to usage reporting and payment, for example, specifying that each purchase of content must be reported to its creator. (ITG, 11/17/96, IT00035863, TD00189J) "Rules and Controls" means any electronic information that directs, enables, specifies, describes, and/or provides contributing means for performing or not-performing, permitted and/or required operations related to Content, including, for example, restricting or otherwise governing the performance of operations, such as, for example, Management of such Content. (License Agreement: IT and Universal Music Group, 4/13/99, Exhibit 11 to InterTrust 30(b)(6)) Que at 348; Webster's New World Dictionary of Computer Terms (4th ed.) at 365
secure 193.1, 193.11, 193.15, 912.35, 861.58, 891.1, 683.2, 721.34	Intrinsic: Because this term is indefinite and used inconsistently, each use of "secure" and forms thereof in the asserted patents is relevant and herein included by reference. The following examples are illustrative. - "HPEs 655 may be provided in two types: secure and not secure." ('193 80:8-9) - "Because secondary storage 652 is not secure, SPE 503 must encrypt and cryptographically seal (e.g., using a one-way hash function initialized with a secret value known only inside the SPU 500) each swap block before it writes it to secondary storage." ('193 107:39-42) - "Insecure external memory may reduce the wait time for swapped pages to be loaded into SPU 500, but will still incur substantial encryption/decryption penalty for each page." ('193 125:56-59) - "The following is a non-exhaustive list of some of the advantageous features provided by ROS 602 in the preferred embodiment: ... Secure secure communications secure control functions secure virtual memory management information control structures protected from exposure data elements are validated, correlated and access controlled components are encrypted and validated independently components are tightly correlated to prevent unauthorized use of elements control structures and secured executables are validated prior to use to protect against tampering integrates security considerations at the I/O level provides on-the-fly decryption of information at release time enables a secure commercial transaction network flexible key management features" ('193 72:52, 73:19) - "ROS 602 generates component assemblies 690 in a secure matter. As shown graphically, in FIGS. 11I and 11J, the different elements comprising a component assembly 690 may be "interlocking" in the sense that they can only go together in ways that are intended by the VDE participants who created the elements and/or specified the component assemblies. ROS 602 includes security protections that can prevent an unauthorized person from modifying elements, and also prevent an unauthorized person from substituting elements." (82:60) - - "Because of VDE security, including use of effective encryption, authentication , digital signature, and secure database structures, the records contain within a VDE card arrangement may be accepted as valid transaction records for government and/or corporate recordkeeping requirements." (19:49) - "In order to maintain security, SPE 503 must encrypt and cryptographically seal each block being swapped out to a storage device external to a supporting SPU 500, and must similarly decrypt, verify the cryptographic seal for, and validate each block as it swapped into SPU 500." (123:60) - "As mentioned above, memory external to SPU 500 may not be secure. Therefore, when security is required, SPU 500 must encrypt secure information before writing it to external memory before using it." (69:29) - "Only those processes that execute completely within SPEs 503 (and in some cases, HPEs 655) may be considered to be truly secure. Memory and other resources external to SPE 503 and HPEs 655 used

Claim Term	MS Construction
	to store and/or process code and/or data to be used in secure processes should only receive and handle that information in encrypted form unless SPE 503/HPE 655 can protect secure process code and/or data form non-secure processes." (79:11) - "From time to time, two parties (e.g., PPEs A and B), will need to establish a communication channel that is know by both parties to be secure form eavesdropping, secure from tampering, and to be in use solely by the two parties whose identifies are correctly known to each other." (215:35) - "Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed form outside observation and interference, the present invention ensures that content control information can be enforced." ('193 46:4-8) '193 199:38-47, 221:1-21 See also prior art referenced in the relevant file histories, e.g. Stefik; Tygar et al., "Dyad: A System for Using Physically Secure Coprocessors," School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213 (May 1991). Extrinsic: "No data system can be made secure without physical protection of some part of the equipment." (Davies, p. 3)[9] "Security is a negative attribute. We judge a system to be secure if we have not been able to design a method of misusing it which gives some advantage to the attacker." (Davies, p.4) "Various criteria exist for secure systems - U.S. Dept. of Defense Trusted Computer Security Evaluation Criteria (TCSEC), the Orange Book, Red Book, European and Canadian guidelines, U.S. National Institute of Standards and Technology, and United Kingdom guidelines." (Neumann)[10] "Security: 1. Protection against unwanted behavior. In present usage, computer security includes properties such as confidentiality, integrity, availability, prevention of denial of service and prevention of generalized misuse. 2. The property that a particular security policy is enforced, with some degree of assurance. 3. Security is sometimes used in the restricted sense of confidentiality, particularly in the case of multilevel security. Multilevel Security - A confidentiality policy based on the relative ordering of multilevel security labels (really multilevel confidentiality, ex. - no adverse flow of information with respect to sensitivity of information)" (Neumann, Glossary) "There are two principal objectives: secrecy (or privacy), to prevent unauthorized disclosure of data; and authenticity or integrity) [sic], to prevent the unauthorized modification of data. ... Note, however, that whereas it can be used to detect message modification, it cannot prevent it. Encryption alone does not protect against replay, because an opponent could simply replay previous ciphertext." (Denning, p.5) "A cipher in unconditionally secure if, no matter how much ciphertext is intercepted, there is not enough information in the ciphertext to determine the plaintext uniquely." (Denning, p.5) (Davies, p. 41, 380) "A cipher is computationally secure, or strong, if it cannot be broken by systematic analysis with available resources." (Denning, p.5) (Davies, p.41, 370) Security: The combination of integrity and secrecy, applied to data. (ITG, 5/12/95, IT00028295) Secrecy: The inability to obtain any information from data. (ITG, 5/12/95, IT00028294) ". . . security includes concealment, integrity of messages, authentication of one communicating party by the other. . ." (Neumann, p. 8)

[9] "Davies" herein refers to Davies, D., et al, Security for Computer Networks, 1984.
[10] "Neumann" herein refers to Neumann, P.G., Computer Related Risks, 1995

Claim Term	MS Construction
	"Computer security rests on confidentiality, integrity, and availability. The interpretations of these three aspects vary, as do the contexts in which they arise. Confidentiality is the concealment of information or resources. [] Confidentiality also applies to the existence of data, which is sometimes more revealing than the data itself. [] All mechanisms that enforce confidentiality require supporting services from the system. The assumption is that the security services can rely on the kernel, and other agents, to supply correct data. Thus, assumptions and trust underlie the confidentiality mechanisms. Integrity refers to the trustworthyness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the informationz) and origin integrity (the source of the data, often called authentication). Integrity mechanisms fall into two classes: prevention mechanisms and detection mechanisms. Protection mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways. Detection mechanisms do not try to prevent violations of integrity; they simple report that the data's integrity in no longer trustworthy." (Bishop, p. 4-6)[11] "Definition 4-1. A security policy is a statement that partitions the states of the system into a set of authorized, or secure, states and a set of unauthorized, or nonsecure, states. Definition 4-2. A secure system is a system that starts in an authorized state and cannot enter an unauthorized state." (Bishop, p. 95) "24.5.1 Secure Systems Systems designed with security in mind have auditing mechanisms integrated with the system design and implementation." (Bishop, p.706) "Computer security is assuring the secrecy, integrity, and availability of components of computing systems. The three principal pieces of a computing system subject attacks are hardware, software, and data. These three pieces, and the communications between them, constitute the basis of computer security vulnerabilities. This chapter has identified four kinds of attacks on computing systems: interruptions, interceptions, modifications, and fabrications. Three principles affect the direction of work in computer security. By the principle of easiest penetration, a computing system penetrator will use whatever means of attack is the easiest; therefore. All aspects of computing system security need to be considered at once. By principle of timeliness, a system needs to be protected against penetration only long enough so that penetration is of no value to the penetrator. The principle of effectiveness states that controls must be usable and used in order to serve purpose. Controls can be applied at the levels of data, programs, the system, physical devices, communications links, the environment, and personnel. Sometimes several controls are needed to cover a single vulnerability, and sometimes one control addresses several problems at once." (Pfleeger, p.4) See also InterTrust's Rule 30(b)(6) testimony and Microsoft PLR 4-2 Exhs. E & F as revised. (Examples follow). Webster's New 20th century Dictionary (1947) at 1540-41); Pfleeger at 4-5; Spencer, Personal Computer Dictionary at 156; The Computer Glossary at 460; McGraw-Hill Dictionary of Scientific and Technical Terms at 1788; Practical Unix Security at 11-12 (O'Reilly 1991); Bishop, Computer Security (2002) pp. 3-24, 47; Hoffman, Modern Methods for Computer Security and Privacy at 2, 134-35; Mullender, ed., Distributed Systems (Addison Wesley 2d ed.) at 367, 420; Landewehr, "Formal Models for Computer Security" (ACM 1981); Merkle, "Protocols for Public Key Cryptosystems" (IEEE 1980); Cooper, Computer & Communication Security, at 383; Baker, The Computer Security Handbook at 273; Computer Security Handbook at 389; Matheson et al., Robustness and Security of Digital Watermarks;

[11] ``Bishop'' herein refers to ``Bishop, M., Computer Security, Art & Science, 2003).

Claim Term	MS Construction
	National Information Systems Security (INFOSEC) Glossary at 49-50; Internet Security Glossary (RFC2828); Tanenbaum, Modern Operating Systems (1992) at 181-82 IN64706-45, IN176319-72, IT735936 (integrity), IT735938-9 IN00862862, IT1678-96, IT39208-26, IT702969-83, IT399877-80 "Secure. Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user."; "Computer Security. 1. Concepts, techniques, technical measures, and administrative measures used to protect the hardware, software and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification or use or loss. 2. Protection resulting from the application of computer security." (IBM) "Security: Freedom from risk or danger. Safety and assurance of safety"; "secure state - a condition in which none of the subjects in a system can access objects in an unauthorized manner. . ."(Russell, Computer Security Basics, 1992, pp. 8-11, 113, 227, 420) "Various criteria exist for secure systems - U.S. Dept. of Defense Trusted Computer Security Evaluation Criteria (TCSEC), the Orange Book, Red Book, European and Canadian guidelines, U.S. National Institute of Standards and Technology, and United Kingdom guidelines." The New IEEE Standard Dictionary of Electrical and Electronics Terms, 5th Ed. (1993) at 1181 ("The protection of computer hardware and software from accidental or malicious access, use, modification, destruction, or disclosure.") Dictionary of Computing, 3rd Ed. (1990) at 406 ("Prevention of or protection against (a) access to information by unauthorized recipients or (b) intentional but unauthorized destruction or alteration of that information.") Information Security Dictionary of Concepts, Standards, and Terms (1992) ("The quality or state of being cost-effectively protected from undue losses (e.g. loss of goodwill, monetary loss, loss of ability to continue operations, etc.)")
secure container 912.35, 861.58, 683.2	See "secure" and "container" Intrinsic: - Prosecution History of '861 Patent: "Anderson [U.S. Patent No. 5,537,526] does not explicitly address a secure container *per se*, but does place documents into containers [Fig. 8 202] and place restriction via links attached to documents ... which can include restrictions ... Such security tools are rightfully attached to a structure encapsulating the document, e.g. its container." 08/805,804 ('861), Office Action, 06/25/98, p. 5. MSI 27417-25 - Prosecution History of '683 Patent: "Claims 7-11, ... are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (5,412,717) in view of Narasimhalu et al (5,499,298). ... The set of authorities and restrictions are referred to as "program authorization information" or "PAI". ... A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... Here, Fischer provides a secure container in the form of a program, i.e. a governed item, having an associated PAI, i.e. at least one rule associated with the secure container." 09/221,479('683), Office Action, 11/12/99, p. 3-4 (IT00065799-800 in IT65863-65) - Prosecution History of Application 08/689,606, filed 12 August 1996: (issued as USP 5,943,422 incorporating '107) Amendment dated 2 July 1998: "1. (Amended) A rights management method comprising: (a) receiving an information signal; (b) steganographically decoding the received information signal to recover digital rights management control information packaged within at least one secure digital container; and (c) performing at least one rights management operation based at least in

Claim Term	MS Construction
	part on the recovered digital rights management control information. [] Remarks [] For example, amended Claims 1, 15 and 22 each recite a digital secure container in combination. Neither Rhoads [USP 5,636,292], nor any of the other applied references, teaches or suggests the recited combination of features including any digital secure container." - Rhoads, USP 5,636,292: "Fully Exact Steganography Prior art steganographic methods currently known to the inventor generally involve fully deterministic or "exact" prescriptions for passing a message. Another way to say this is that it is a basic assumption that for a given message to be passed correctly in its entirety, the receiver of the information needs to receive the exact digital data file sent by the sender, tolerating no bit errors or "loss" of data. By definition, "lossy" compression and decompression on empirical signals defeat such steganographic methods. (Prior art, such as the previously noted Komatsu work, are the exceptions here.) The principles of this invention can also be utilized as an exact form of steganography proper. It is suggested that such exact forms of steganography, whether those of prior art or those of this invention, be combined with the relatively recent art of the "digital signature" and/or the DSS (digital signature standard) in such a way that a receiver of a given empirical data file can first verify that not one single bit of information has been altered in the received file, and thus verify that the contained exact steganographic message has not been altered. " (55:5-26) "One exemplary application is placement of identification recognition units directly within modestly priced home audio and video instrumentation (such as a TV). Such recognition units would typically monitor 'audio and/or video looking for these copyright identification codes, and thence triggering simple decisions based on the findings, such as disabling or enabling recording capabilities, or incrementing program specific billing meters which are transmitted back to a central audio/video service provider and placed onto monthly invoices." (29:23) - "Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility." ('683 8:50-52) - "Even if the object is stored locally to the VDE node, it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object." ('193 192:41-) - "Electronic delivery person 4060 receives item 4054 in digital form and places it into a secure electronic container 302--thus forming a digital "object" 300. A digital object 300 may in this case be, for example, as shown in FIGS. 5A and 5B, and may include one or more containers 302 containing item 4054. FIG. 88 illustrates secure electronic container 302 as an attaché case handcuffed to the secure delivery person's wrist. Once again, container is shown as a physical thing for purposes of illustration only--in the example it is preferably electronic rather than physical, and comprises digital information having a well-defined structure (see FIG. 5A). Special mathematical techniques known as "cryptography" can be used to make electronic container 302 secure so that only intended recipient 4056 can open the container and access the electronic document (or other item) 4054 it contains." ('683 15:56-16:6) - "Because container 152 can only be opened within a secure protected processing environment 154 that is part of the virtual distribution environment described in the above-referenced Ginter et al. patent disclosure" ('712 168:22-25) - "A VDE content container is an object that contains both content (for example, commercially distributed electronic information products such as computer software programs, movies, electronic publications or reference materials, etc.) and certain control information related to the use of the object's content." ('193 19:15-21) - ('193 82:24-45); ('193 192:36-52); ('683 18:49-56);('861 4:51-64) Extrinsic: Container: VDE objects are represented in a special form called a container. The container is

Claim Term	MS Construction
	implemented within the VDE as an object-oriented container class. The container class provides a standard method by which applications software may encapsulate and read information stored within the object. Additionally, the container may include procedural information associated with the data being stored. Containers may be nested, and share attributes with nested elements. Nested containers are stored within a larger container. VDE recognizes the presence of additional objects within the content, and allows the nested containers to share, extend or override the attributes of an outer container. (VDE ROI DEVICE v1.0a 9 Feb 1994, IT00008572) Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Container: In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers. (Longley) Container: A protected (encrypted) storage object that incorporates descriptive information, protected content, and (optionally) control objects applicable to that content. (ITG, 3/7/1995, IT00709617, see footnote 2) Container: A contains protected *content*, which is divided into one or more *atomic elements*, and, optionally, *PERCs* governing the *content* and may be manipulated only as specified by a *PERC*. (ITG, 4/6/95, IT00028206, see footnote 5) Container: A packaging mechanism, consisting of: *One or more Element-derived components. *An organization mechanism which provides a unique name within a flat namespace for each of the components in a Container (ITG, 5/12/95, IT00028293) Container: A protected digital information storage and transport mechanism for packaging content and control information. (ITG, 8/21/95, IT00032372, TD00068B) "Secure Container(s)" means electronic container(s) or electronic data arrangements that: (I) use one or more cryptographic or other obfuscation techniques to provide protection for at least a portion of the Content thereof; and (ii) supports the use of Rules and Controls to enable the Management of Content. (License Agreement IT and Universal Music Group, 4/13/99, Exhibit 11 to IT 30(b)(6)) A protected digital information storage and transport mechanism for packaging content and control information. (IT 691187) Secure container: A DigiBox container provides security through encryption and the PPE of a commerce node. A secure container does not require a secure communications transport mode. (IT 35965) A DigiBox container provides for the persistent protection of its properties. (IT 35920) DigiBox containers ensure integrity. (IT 35895)
secure container governed item 683.2	Intrinsic: Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Container: In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers. (Longley) Item: 1. An element of a set of data. 2. One unit of a commodity such as one ox, one bag, or one can. (IBM) Item: In computing, a group of related characters treated as a unit. For example, a record may comprise a number of items, that in turn may consist of other items. (Longley) Container: A protected (encrypted) storage object that incorporates descriptive information, protected content, and (optionally) control objects applicable to that content. (ITG, 3/7/95, IT00709617, see footnote 2) Container: A packaging mechanism, consisting of: *One or more Element-derived components. *An

Claim Term	MS Construction
	organization mechanism which provides a unique name within a flat namespace for each of the components in a Container (ITG, 5/12/95, IT00028293) Container: A protected digital information storage and transport mechanism for packaging content and control information. (ITG, 8/21/95, IT00032372, TD00068B) Secure Processing Unit: The physically secure hardware component of the SPE: a processor with local memory and non-volatile storage. The SPE consists of the SPU itself and the SPE software running on the SPU. (ITG, 3/7/95, IT00709620, see footnote 2) DigiBox Container: InterTrust's secure cryptographic data structure for packaging and containing contents and controls. A DigiBox container provides for the persistent protection of its content and controls through the Protected Processing Environment of XECutor. A DigiBox container eliminates the need for a secure communications channel, such as SSL or SHTTP. (ITG, 10/2/96, IT00035893, TD00189F) DigiBox Container: A format for protected storage and transport of digital content and business rules. The DigiBox container uses cryptography to ensure that the information it holds is protected and can only be manipulated by InterTrust Commerce Nodes. (ITG, 11/17/96, IT00035866, TD00189J)
secure database 193.1, 193.11, 193.15	Intrinsic: - See '193, Figures 7, 10. - "FIG. 36 shows an example of how a new record or element may be inserted into a secure database 610. The load process 1070 shown in FIG. 35 checks each data element or item as it is loaded to ensure that it has not been tampered with, replaced or substituted. In the process 1070 shown in FIG. 35, the first step that is performed is to check to see if the current user of electronic appliance 600 is authorized to insert the item into secure database 610 (block 1072)... The non-secure element within its security wrapper may then be stored within secure databases 610." - "The keys to decrypt secure database 610 records are, in the preferred embodiment, maintained solely within the protected memory of an SPU 500." - "By using this process, SPE 503 can protect the data structure (including the indexes) of secure databases 610 against substitutions of old items and against substitution of indexes for current items." - "The security of secure databases 610 files may be further improved by segmenting the records into "compartments." Different encryption/decryption keys may be used to protect different "compartment." This strategy can be used to limit the amount of information within secure database 310 that is encrypted with a single key/ Another technique for increasing secure database 610 may be to encrypt different portions of the same records with different keys so that more than one key may needed to decrypt these records." - "Each electronic appliance 600 may have an instance of secure database 610 that securely maintains the VDE items. FIG. 16 shows one example of a secure database 610. - "VDE Secure Database 610: VDE 100 stores separately deliverable VDE elements in a secure (e.g., encrypted) database 610 distributed to each VDE electronic appliance 610. The database 610 in the preferred embodiment may store and/or manage three basic classes of VDE items: VDE objects, VDE process elements, and VDE data structures." - "Secure Database Keys: PPE 650 preferably generates these secure database keys and never exposes the outside of the PPE. They are site-specific in the preferred embodiment, and may be "aged" as described above. As described above, each time an updated record is written to secure database 610, a new key may be used and kept in a key list within the PPE." (212:36) - "Secure database encryption keys in the preferred embodiment are frequently changing and are also site specific." (219:30) - ('193 79:24); ('193 71:28-40); ('193 111:59-67)

Claim Term	MS Construction
	Extrinsic: Secure store: The Secure store is the system area that provides an encrypted storage method for storing ROI internal files and other highly secure information. In some applications, entire media volumes can be distributed encrypted as part of the secure store to enhance overall security for the content by obscuring the file system and media descriptors associated with the volume. A dedicated volume or partition will only be required if an application cannot be supported without it. (e.g. a required government security level for the specific application). In most cases, the user will not be required to dedicate an entire volume or partition of the hard disk, and the secure store will be supported using an encrypted file, or files, on the hard disk. ROI will also support a dedicated partition as an option to the administrator of a network server, as one of several ways to assure the integrity of the system. (VDE ROI DEVICE v1.0a 9 Feb 1994, IT00008586) Database: 1. A collection of data with a given structure for accepting, storing, and providing, on demand, data for multiple users. 2. A collection of interrelated data organized according to a database schema to serve one or more applications. 3. A collection of data fundamental to a system. 4. A collection of data fundamental to an enterprise.(IBM) Database: 1. An extensive and comprehensive set of records collected and organized in a meaningful manner to serve a particular purpose. 2. In computing, a collection of stored operational data used by the applications system of an enterprise. (Longley) "The basic security requirements of data base systems are not unlike the security requirements of other computing systems we have studied. The basic problem-access control, exclusion of spurious data, authentication of users, reliability-have appeared in many context so far in this book. Following is a list of requirements for security of data base systems. Physical data base integrity, so that the data of a data base is immune to physical problems, such as power failures, and so that it is possible to reconstruct that data base if it is destroyed through a catastrophe. Logical data base integrity, so that the structure of the data base is preserved. With logical integrity of a data base, a modification to the value of one field does not affect other field, for example. Element integrity, so that the data contained in each element is accurate. Auditability, to be able to track who has accessed (or modified) the elements in the data base. Access control, so that a user is allowed to access only authorized data and so that different user can be restricted to different modes of access (for example, read or write). User authentication, to be sure that every user is positively identified, both for audit trail and for permission to access data. Availability, meaning that users can access the data base in general and all the data for which they are authorized." (Pfleeger) Security: The combination of integrity and secrecy, applied to data. (ITG, 5/12/95, IT00028295) Secrecy: The inability to obtain any information from data. (ITG, 5/12/95, IT00028294)
secure execution space 721.34	Intrinsic: - Prosecution History of '721 Patent : "execution spaces" "refers to a resource which can be used for execution of a program or process." Amendment - - "Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. Tamper resistant barriers may be used to protect this programming or other conditioning. The assurance levels described below are a measure or assessment of the effectiveness with which this programming or other conditioning is

Claim Term	MS Construction
	protected." - ('721 3:16-23) - - "A protected processing environment or other secure execution space protects itself by executing only those load modules or other executables that have been digitally signed for its corresponding assurance level." - "Different protected processing environments (secure execution spaces) might examine different subsets of the multiple digital signatures--so that compromising one protected processing environment (secure execution space) will not compromise all of them." - "The internal ROM 532 and RAM 534 within SPU 500 provide a secure operating environment and execution space." ('193 69:33-35) - SPU 500 general purpose RAM 534 provides, among other things, secure execution space for secure processes. ('193 70:43-44) - "Virtual memory manager 580 provides a fully "virtual" memory system to increase the amount of "virtual" RAM available in the SPE secure execution space beyond the amount of physical RAM 534a provided by SPU 500." ('193 109:24-45) Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Execution: The process of carrying out an instruction or instructions of a computer program by a computer. (IBM) Space: 1. A site intended for storage of data. 2. A basic unit of area, usually the size of a singe character. 8. To cause a printer to move the paper a specified number of lines either before or after it prints a line. (IBM)
secure memory, memory 193.1, 193.11, 193.15	Intrinsic: - "Because secondary storage 652 is not secure, SPE 503 must encrypt and cryptographically seal (e.g., using a one-way hash function initialized with a secret value known only inside the SPU 500) each swap block before it writes it to secondary storage." ('193 107:39-46) - "Due to the practical limits on the amount of ROM 532 and RAM 534 that may be included within SPU 500, SPU 500 may store information in memory external to it, and move this information into and out of its secure internal memory space on an as needed basis." ('193 18:14-19); - "Such external memory may be used to store SPU programs, data and/or other information. For example, a VDE control program may be, at least in part, loaded into the memory and communicated to and decrypted within SPU 500 prior to execution. Such control programs may be re-encrypted and communicated back to external memory where they may be stored for later execution by SPU 500. "Kernel" programs and/or some or all of the non-kernel "load modules" may be stored by SPU 500 in memory external to it. Since a secure database 610 may be relatively large, SPU 500 can store some or all of secure database 610 in external memory and call portions into the SPU 500 as needed. As mentioned above, memory external to SPU 500 may not be secure. Therefore, when security is required, SPU 500 must encrypt secure information before writing it to external memory, and decrypt secure information read from external memory before using it. Inasmuch as the encryption layer relies on secure processes and information (e.g., encryption algorithms and keys) present within SPU 500, the encryption layer effectively "extends" the SPU security barrier 502 to protect information the SPU 500 stores in memory external to it." ('193 71:19-40) - "Key and Tag Manager 558 also provides services relating to tag generation and management. In the preferred embodiment, transaction and access tags are preferably stored by SPE 503 (HPE 655) in protected memory (e.g., within the NVRAM 534b of SPU 500). These tags may be generated by key and tag manager 558. They are used to, for example, check access rights to, validate and correlate data elements. For example, they may be used to ensure components of the secured data structures are not

Claim Term	MS Construction
	tampered with outside of the SPU 500." ('193 120:59-121:1) - "The degree of overall security of the VDE system is primarily dependent on the degree of tamper resistance and concealment of VDE control process execution and related data storage activities. Employing special purpose semiconductor packaging techniques can significantly contribute to the degree of security. Concealment and tamper-resistance in semiconductor memory (e.g., RAM, ROM, NVRAM) can be achieved, in part, by employing such memory within an SPU package, by encrypting data before it is sent to external memory (such as an external RAM package) and decrypting encrypted data within the CPU/RAM package before it is executed. This process is used for important VDE related data when such data is stored on unprotected media, for example, standard host storage, such as random access memory, mass storage, etc." ('193 21:26-40) - "Secondary storage 662 may comprise the same one or more non-secure secondary storage devices (such as a magnetic disk and a CD-ROM drive as one example) that electronic appliance 600 uses for general secondary storage functions. In some implementations, part or all of secondary storage 652 may comprise a secondary storage device(s) that is physically enclosed within a secure enclosure. However, since it may not be practical or cost-effective to physically secure secondary storage 652 in many implementations, secondary storage 652 may be used to store information in a secure manner by encrypting information before storing it in secondary storage 652. If information is encrypted before it is stored, physical access to secondary storage 652 or its contents does not readily reveal or compromise the information." ('193 62:43-58) - ('193 59:60-60:3); ('193 69:47-48); ('193 164:55-60); ('193 59:48-59); ('193 63:60-64:5); ('193 69:6-11); ('193 69:27-32); ('193 69:39-43); ('193 71:32-35); ('193 71:42-47); ('193 78:16-17); ('193 120:37-41) Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Memory: All of the addressable storage space in a processing unit and other internal storages that is used to execute instructions.(IBM)
secure operating environment, said operating environment 891.1	Intrinsic: - VDE provides a secure operating environment employing VDE foundation elements along with secure independently deliverable VDE components that enable electronic commerce models and relationships to develop." ('193 13:37-41) - "The internal ROM 532 and RAM 534 within SPU 500 provide a secure operating environment and execution space." (67:29) - ('193 34:26-49); ('193 72:52-73:37); ('193 77:30-44) Extrinsic: Execution environment: Some load modules contain code that executes in a ROI device. Some load modules will contain code that executes in the user's platform microprocessor. This allows methods to be constructed that execute in whichever environment is appropriate. For example an information method could be built to execute only in ROI secure space for government classes of security, or in the user's platform microprocessor for virtually all commercial applications. The public header of the load module will contain a field that indicates where it needs to execute. This functionality also allows for different ROI devices as well as different user platforms and allows methods to be constructed for either. It should be noted that load modules that execute outside of an ROI device are deemed insecure by the VDE Architecture and secure processes should not be implemented using load modules that execute outside of an ROI device. (VDE ROI DEVICE v1.0a, 9 Feb 1994, IT00008592) "Saltzer [SAL74] and Saltzer and Schroeder [SAL75] listed the following principles of the design of secure protection systems. Least privilege: Each user and each program should operate using the fewest privileges

Claim Term	MS Construction
	possible. In this way, the damage from an inadvertent or malicious attack is minimized. Economy of mechanism: The design of the protection system should be small, simple and straightforward. Such a protection can be exhaustively tested, perhaps verified, and trusted. Open design: The protection mechanism must not depend on the ignorance of potential attackers; the mechanism should be public, depending on secrecy of relatively few key items, such as a password table. An open design is also available for extensive public scrutiny. Complete mediation: Every access must be checked. Permission-based: The default condition should be denial of access. A conservative designer identifies those items that should be accessible, rather than those that should not. Separation of privilege: Ideally, access to objects should depend on more than one condition, such as user authentication plus a cryptographic key. In this way, someone who defeats one protection system will not have complete access. Least common mechanism: Shared objects provide potential channels for information flow. Systems employing physical or logical separation reduce the risk from sharing. Easy to use: If a mechanism is easy to use, it is unlikely to be avoided." (Pfleeger section 7.2) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment.* (ITG, 8/21/95, IT00032375, TD00068B)
securely applying 891.1	Intrinsic: Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Applying: 1. In journaling, to place after-images of records into a physical file member. The after-images are recorded as entries in a journal. 2. An SMP process that moves distributed code and MVS-type programs to the system libraries. (IBM)
securely assembling 912.8, 912.35	Intrinsic: - ('193 87:33-40) - "ROS 602 also provides a tagging and sequencing scheme that may be used within the loadable component assemblies 690 to detect tampering by substitution. ('193 87:41-62) - "ROS 602 generates component assemblies 690 in a secure manner. As shown graphically in FIGS. 11I and 11J, the different elements comprising a component assembly 690 may be "interlocking" in the sense that they can only go together in ways that are intended by the VDE participants who created the elements and/or specified the component assemblies. ROS 602 includes security protections that can prevent an unauthorized person from modifying elements, and also prevent an unauthorized person from substituting elements." ('193 84:60-85:2) - "ROS 602 assembles these elements together into an executable component assembly 690 prior to loading and executing the component assembly (e.g., in a secure operating environment such as SPE 503 and/or HPE 655). ROS 602 provides an element identification and referencing mechanism that includes information necessary to automatically assemble elements into a component assembly 690 in a secure manner prior to, and/or during, execution." ('193 83:44-52) - ('107 page 782 claim 80); ('193 116:25-35); ('193 116:29-33) Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM)

Claim Term	MS Construction
securely processing 891.1	Intrinsic: - "VDE can satisfy the requirements of widely differing electronic commerce and data security applications by, in part, employing this general purpose transaction management foundation to securely process VDE transaction related control methods." ('193 25:52-57) - "For example, they [HPE and SPE] may each perform secure processing based on one or more VDE component assemblies 690, and they may each offer secure processing services to OS kernel 680." ('193 79:43-46) - "VDE methods 1000 are designed to provide a very flexible and highly modular approach to secure processing." ('193 181:18-19) - "In these cases, secure processing steps performed by an SPU typically must be segmented into small, securely packaged elements that may be "paged in" and "paged out" of the limited available internal memory space." (67:39) - ('193 21:43-22:31); ('193 109:24-45); ('193 139:28-31); ('683 24:26-33) - Load modules are not necessarily directly governed by PERCs 808 that control them, nor must they contain any time/date information or expiration dates. The only control consideration is the preferred embodiment is that one or more methods 1000 reference them using a correlation tag (the value of a protected object created by the load module's owner, distributed to authorized parties for inclusion in their methods, and to which access and use is controlled by one or more PERCs 808). If a method core 1000' references a load module 1100 and asserts the proper correlation tag (and the load module satisfies the internal tamper checks for the SPE 503), then the load module can be loaded and executed, or it can be acquired from, shipped to, updated, or deleted by, other systems. - ROS 602 also provides a tagging and sequencing scheme that may be used within loadable component assemblies 690to detect tampering by substitution. Each element comprising a component assembly 690 may be loaded into a SPU 500, decrypted using encrypt/decrypt engine 522, and then tested/compared to ensure that the proper element has been loaded. ...In addition, a validation/correlation tag stored under the encrypted layer of the loadable element may be compared to make sure it matches on or more tags provided by a requesting process. This prevents unauthorized use of information. As a third protection, a device assigned tag (e.g., a sequence number) stored under an encryption layer of loadable element may be checked to make sure it matches a corresponding tag value expected by SPU 500. This prevents substitution of older elements. Validation/correlation tags are typically passed only in secure wrappers to prevent plaintext exposure of this information outside of SPU 500.. - Key and Tag Manager 558 also provides service relating to tag generation and management. In the preferred embodiment, transaction and access tags are preferably stored by SPE 503 (HPE 665) in protected memory (e.g., within the NVRAM 534b of SPU 500). These tags may be generated by key and tag manager 558. They are used to, for example, check access rights to, validate and correlate data elements. For example, they may be used to ensure components of the secured data structures are not tampered with outside of the SPU 500. - Initiation of load module execution in this environment is strictly controlled by a combination of access tags, validation tags, encryption keys, digital signatures, and/or correlation tags. Thus, a load module 1100 may only be referenced if the caller knows it ID and asserts the shared secret correlation tag specific to that load module. The decrypting SPU may match the identification token an and local access tag of a load module after decryption. These techniques make the physical replacement of any load module 1100 detectable at the next physical access of a load module. - Meters and budgets are common examples of this. Expiration dates cannot be used effectively to prevent substitution of the previous copy of a budget UDE 1200. To secure these frequently updated items, a transaction tag is generated and included in the encrypted item each time that item is updated. A list of all VDE items Ids and the current transaction tags for each item is maintained as part of the secure database 610. UDEs 1200 are preferably encrypted using a site specific key once they are loaded into a site. This site-specific key marks a validation tag that may be derived from a cryptographically strong pseudo-random

Claim Term	MS Construction
	sequence by the SPE 503 and updated each time the record is written back to the secure database 610. This technique provided reasonable assurance that the UDE 1200 has not been tampered with nor submitted when it is requested by the system for the next use. Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Process: 1. The performance of logical operations and calculations on datum including temporary retention of data in processor storage while the data is being operated on. (IBM) Process: Process: (1) in computing, the active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. (2) In computing, a program in execution. . . .(4) In computing, a program is a static piece of code and a process is the execution of that code. (Longley) Processing: In legislation, as defined by the U.K. Data Protection Act o f 1984, pertaining to the amending, augmenting, deleting, or re-arranging of the data or extracting the information constituting the data and , in the case of personal data, processing means performing any of the abovementioned operations by reference to the data subject. (Longley)
securely receiving 891.1	Intrinsic: Prosecution History of Application 08/388,107: "Johnson's user database is not securely delivered, but rather is created at the license server by--and is under the control of--the site administrator." 08/388,107, Amendment, 06/20/97, p. 23 (MSI028847) "[A]pplicants' independent claims ... require secure delivery of both first and second control items originating from someplace other than the appliance where they are used, at least in part, for controlling the same process, operation or the like. This feature in combination is not taught or suggested by Johnson and/or Rosen." (pg. 23) "Johnson's user database is not securely delivered, but rather is created at the license server by--and is under the control of--the site administrator." (pg. 23) "Rosen does not disclose or suggest securely delivering controls of plural different entities and/or appliances from at least one source remote to the receiving site or appliance as recited in applicants' independent claims ...., Rosen's is distinguishable at least because Rosen's merchant trusted agent (MTA) and customer trusted agent (CTA) are loaded into different appliances and operate in different appliances. ... Furthermore, such loading operation is performed at Rosen's physically secure device manufacturing site -- not from at least one source remote to the device." (pg. 23-24) 08/388,107, Amendment, 06/20/97, p. 23, 23, 24 (MSI028847-48) - "Secure communications means employing authentication, digital signaturing, and encrypted transmissions." ('193 12:5-35, 12:33) - The appliance 600 may then open the secure electronic container ("attaché case") 302 and deliver the item it contains to recipient 4056 (FIG. 91B, block 4092D). ('683) - "FIGS. 114A-118 show example processes for securely receiving an item" ('683 14:64-65) - "By way of non-exhaustive summary, these present inventions provide a highly secure and trusted item delivery and agreement execution services providing the following features and functions:" ('683:6) - "When encrypted or otherwise secured information is delivered into a user's secure VDE processing area (e.g., PPE 650), a portion of this information can be used as a "tag" that is first decrypted or otherwise unsecured and then compared to an expected value to confirm that the information represents

Claim Term	MS Construction
	expected information. The tag thus can be used as a portion of process confirming the identity and correctness of received, VDE protected, information." (214:17) - "For objects in which maintaining security is particularly important, the permission records 808 and key blocks 810 will frequently be distributed electronically, using secure communications techniques (discussed below) that are controlled by the VDE nodes of the sender and receiver." ('193 129:8-13) - "Creator B ... may accept such a [new control] model if information associated with the one or more meter methods that record the number of bytes decrypted by users is securely packaged by distributor B's VDE secure subsystem and is securely, employing VDE communications techniques, sent to creator B in addition to distributor A" ('193 307:46-51) - ('193 209:27-30); ('193 29:64-30:4); ('193 36:29-33); ('193 45:39-45); ('193 153:53-67); ('193 293:4-7); ('683 15:67-16:4) Extrinsic: Secure: Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user. (IBM) Receiving: 1. To obtain and store data.(IBM) Secure Processing Unit: The physically secure hardware component of the SPE: a processor with local memory and non-volatile storage. The SPE consists of the SPU itself and the SPE software running on the SPU. (ITG, 3/7/1995, IT00709620, see footnote 2)
security level, level of security 721.1; 721.34, 912.8	Intrinsic: - ('193 21:26-31); ('193 45:52-59), but only as to 912.8. - "For example, protected processing environments or other secure execution spaces that are more impervious to tampering (such as those providing a higher degree of physical security) may use an assurance level that isolates it from protected processing environments or other secure execution spaces that are relatively more susceptible to tampering (such as those constructed solely by software executing on a general purpose digital computer in a non-secure location)." - "The present invention may use a verifying authority and the digital signatures it provides to compartmentalize the different electronic appliances depending on their level of security (e.g., work factor or relative tamper resistance)." - "Assurance level I might be used for an electronic appliance(s) 61 whose protected processing environment 108 is based on software techniques that may be somewhat resistant to tampering. An example of an assurance level I electronic appliance 61A might be a general purpose personal computer that executes software to create protected processing environment 108. An assurance level II electronic appliance 61B may provide a protected processing environment 108 based on a hybrid of software security techniques and hardware-based security techniques. An example of an assurance level II electronic appliance 61B might be a general purpose personal computer equipped with a hardware integrated circuit secure processing unit ("SPU") that performs some secure processing outside of the SPU (see Ginter et al. patent disclosure FIG. 10 and associated text). Such a hybrid arrangement might be relatively more resistant to tampering than a software-only implementation. The assurance level III appliance 61C shown is a general purpose personal computer equipped with a hardware-based secure processing unit 132 providing and completely containing protected processing environment 108 (see Ginter et al. FIGS. 6 and 9 for example). A silicon-based special purpose integrated circuit security chip is relatively more tamper-resistant than implementations relying on software techniques for some or all of their tamper-resistance." ('721 __) - "Assurance level in this example may be assigned to a particular protected processing environment 108 at initialization (e.g., at the factory in the case of hardware-based secure processing units). Assigning assurance level at initialization time facilitates the use of key management (e.g., secure key exchange protocols) to enforce isolation based on assurance level. For example, since establishment of assurance level is done at initialization time, rather than in the field in this example, the key exchange

Claim Term	MS Construction
	mechanism can be used to provide new keys (assuming an assurance level has been established correctly)." ('721 __) - "The assurance level III appliance 61C shown is a general purpose personal computer equipped with a hardware-based secure processing unit 132 providing and completely containing protected processing environment 108 (see Ginter et al. FIGS. 6 and 9 for example). A silicon-based special purpose integrated circuit security chip is relatively more tamper-resistant than implementations relying on software techniques for some or all of their tamper-resistance." - "Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. Tamper resistant barriers may be used to protect this programming or other conditioning. The assurance levels described below are a measure or assessment of the effectiveness with which this programming or other conditioning is protected." - SN: 08/689,754: Amendment - Claims 9 and 30 cancelled. - Claims 1-2, 5-6, 10-15, 17-23, 26-27, 31-32, 34, 36, 38-43 amended. Some terms changed (e.g. work factor = security level); points in part to '107 spec'n (and in part to specific portions of '754 app.) to support definiteness of challenged claim terms; "execution spaces" "refers to a resource which can be used for execution of a program or process." (14)); - "In accordance with this feature of the invention, verifying authority 100 supports all of these various categories of digital signatures, and system 50 uses key management to distribute the appropriate verification keys to different assurance level devices. For example, verifying authority 100 may digitally sign a particular load module 54 such that only hardware-only based server(s) 402(3) at assurance level XI may authenticate it. This compartmentalization prevents any load module executable on hardware-only servers 402(3) from executing on any other assurance level appliance (for example, software- only protected processing environment based support service 404(1))." (19:11) - "VDE, in its preferred embodiment, uses special purpose tamper resistant Secure Processing Units (SPUs) to help provide a high level of security for VDE processes and information storage and communication." ('193 4:3-7) - ('193 29:24-28); ('193 49:59-62); ('193 201:51-55); ('193 203:58-67); ('193 212:66-213:15) - "In order to allow, in the preferred embodiment, the ability to differentiate installations with different levels/degrees of trustedness/security, different certification key pairs may be used (e.g., different certification keys may be used to certify SPEs 503 then are used to certify HPEs 655)." (210:36) "security level. To protect digital works against unauthorized uses, repositories need different degrees of physical security. Repositories handling extremely valuable works need greater security than ones for ordinary and portable use. The term security level refers to a sequence of levels ranging from low security to very high security." "Letting Loose the Light: Igniting Commerce in Electronic Publication," Stefik, draft 1994, 1995 (MSI028761) "Security level: Different degrees of physical security – ranging from low security to very high security – for protecting digital works against unauthorized use. Repositories for handling extremely valuable works need greater security than those for ordinary and portable use." "Letting Loose the Light: Igniting Commerce in Electronic Publication," Stefik, in Internet Dreams, MIT 1996 (MSI028785) Prosecution History of '721 Patent: "please amend the application identified above as follows: IN THE CLAIMS Please cancel claims ... and amend claims 1, ... as follows: 1. [Amended] A security method comprising: - (a) digitally signing a first load module with a first digital signature designating the first load

Claim Term	MS Construction
	module for use by a first device class; - (b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and[/or] security level [work factor substantially] different from the at least one of tamper resistance and/[or] security level [work factor] of the first device class; - (c) distributing the first load module for use by at least one device in the first device class; and - (d) distributing the second load module for use by at least one device in the second device class."" (pg. 1-2) "36. [Amended] A protected processing environment comprising: a first tamper resistant barrier having a first security level [work factor], a first secure execution space, and at least one arrangement within the first tamper resistant barrier that prevents the first secure execution space from executing the same executable accessed by a second [further] secure execution space having a second [further] tamper resistant barrier with a second [further] security level [work factor substantially] different from the first security level [work factor]." (pg. 10) "In the pending Office Action, the Examiner rejected claims 1-43 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. By this Amendment, Applicants have canceled claims ... and amended other claims to more appropriately define the present invention. ... In response to the Examiner's rejection, Applicants also have amended Claims 1-2, ... 36, ... to address issues raised by the Examiner." (pg. 13) 08/689,754 ('721), Amendment, 04/14/99, 1-2, 10, 13 Extrinsic: Security: The quality or state of being cost-effectively protected from undue losses (e.g. loss of goodwill, monetary loss, loss of ability to continue operations, etc.) (Longley) Level: 1. The degree of subordination of an item in a hierarchic arrangement. 3. The version of a program. (IBM) Level: 1. In computer security, see security level and integrity level. (Longley) Security level: In computer security, the combination of hierarchical classification and a set of non-hierarchical categories that represent the sensitivity of information. (Longley) Integrity level: In access control, a level of trustworthiness associated with a subject or object. (Longley) Security: The combination of integrity and secrecy, applied to data. (ITG, 5/12/95, IT00028295) Secrecy: The inability to obtain any information from data. (ITG, 5/12/95, IT00028294)
tamper resistance 721.1, 721.34, 900.155	Intrinsic: "The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely." ('193 49:59-62) Extrinsic: Tamper-resistant Module: In data security, a device in which sensitive information, such as a master cryptographic key, is stored and cryptographic functions are performed. The device has one or more sensors to detect physical attacks, by an adversary trying to gain access to the stored information in which case the stored sensitive data is immediately destroyed. (Longley) Information Security Dictionary of Concepts, Standards, and Terms (1992) ("Tamper-resistant Module: In data security, a device in which sensitive information, such as a master cryptographic key, is stored and cryptographic functions are performed. The device has one or more sensors to detect physical

Claim Term	MS Construction
	attacks, by an adversary trying to gain access to the stored information in which case the stored sensitive data is immediately destroyed.") IT41530-49, IT51147-60 Neumann, Computer Related Risks (1995) at 349
Tamper resistant barrier 721.34	Intrinsic: "In addition, Applicants would like to draw the Examiner's attention to other sections of the specification in support of words or phrases cited by the Examiner as "indefinite." ... In claims ... 36 ... the term "barrier" is used as part of the phrase "tamper resistant barrier." This phrase is described in the specification on at least pages 7-8 and 46. In addition, the incorporated Ginter application describes tamper resistant barriers in a number of locations such as, for example, page 201." (pg. 13-14) (pages 7 and 46 of the original specification are '721 2:62-3:13 and 16:35-54 of the issued patent; page 201 of Ginter application SN 08/388,107 is '193 80:40-81:1) 08/689,754 ('721), Amendment, 04/14/99, p. 14 - SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions." ('193 59:48-53) - "Although block 1262 includes encrypted summary services information on the back up, it preferably does not include SPU device private keys, shared keys, SPU code and other internal security information to prevent this information from ever becoming available to users even in encrypted form." ('193 166:59-64) - "Briefly, the preferred example software-based PPE 650 installation process provides the following security techniques: encrypted software distribution, installation customized on a unique instance and/or electronic appliance basis, encrypted on-disk form, installation tied to payment method, unique software and data layout, and identifiable copies." (236:32) - " (c) if the load module has an associate digital signature , authenticating the digital signature at least one public key secured behind a tamper resistant barrier and therefore hidden from the user." ('721.9) - "A further attack technique might involve duplicating one installed operational material 3472 instance by coping the programs and data from one personal computer 3372B to another personal computer 3372C or emulator (see FIG. 67B, block 3364, and the "copy" arrow 3364A in FIG. 67A). The duplicated PPE instance could be used in a variety of ways, such as, for example, to place an imposter PPE 650 instance on-line and/or to permit further dynamic analysis." ('900 233:8-15) - "Various software protection techniques detailed above in connection with FIG. 10 may provide software-based tamper resistant barrier 674 within a software-only and/or hybrid software/hardware protected processing environment 650. The following is an elaboration on those above-described techniques. These software protection techniques may provide, for example, the following: An on-line registration process that results in the creation of a shared secret between the registry and the PPE 650 instance—used by the registry to create content and transactions that are meaningful only to specific PPE instance. An installation program (that may be distinct from the PPE operational material software) that creates a customized installation of the PPE software unique to each PPE instance and/or associate electronic appliance 600. Camouflage protections that make it difficult to reverse engineer the PPE 650 operational materials during PPE 650 operation. Integrity checks performed during PPE 650 operation (e.g., during on-line interactions with trusted servers) to detect compromise. In general, the software-based tamper resistant barrier 674 may establish "trust" primarily through uniqueness and complexity." ('900 235:30-57)- - ('900 243:3-9); ('193 80:40-65, Fig. 10); ('900 230:61-65); ('900 233:24-33); ('900 235:30-56); ('900 236:9-15)

Claim Term	MS Construction
	Extrinsic: Tamper-resistant Module: In data security, a device in which sensitive information, such as a master cryptographic key, is stored and cryptographic functions are performed. The device has one or more sensors to detect physical attacks, by an adversary trying to gain access to the stored information in which case the stored sensitive data is immediately destroyed. (Longley) "The "tamper-resistant module" is physically strong and destroys secrets when opened, and the software running inside has been checked for integrity;" (Davies) "The host computer is provided with a specially, physically secure module containing all the secret information which must be protected. In the IBM papers it is called the 'Cryptographic Facility': we shall call it a 'Tamper Resistant Module' (TRM)." (Davies)
tamper resistant software 900.155	Intrinsic: "Operational materials 3472 may then decrypt the next program segment dynamically ... This mechanism increases the tamper-resistance of the executable code--thus providing additional tamper resistance for PPE operations." ('900 243:3-8) Extrinsic: Tamper-resistant Module: In data security, a device in which sensitive information, such as a master cryptographic key, is stored and cryptographic functions are performed. The device has one or more sensors to detect physical attacks, by an adversary trying to gain access to the stored information in which case the stored sensitive data is immediately destroyed. (Longley) "Tamper resistant software resists observation and modification." Aucsmith, D., Tamper Resistant Software, 1st Workshop on Information Hiding, May 30, 1996.
use 912.8, 912.35, 861.58, 193.19, 891.1, 683.2, 721.1	Intrinsic: - Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving. - Content (executables for example) delivered with proof of delivery and/or execution or other use. - "In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:24-30) - "Some or all of the back up files may be packaged within an administrative object and transmitted for analysis, transportation, or other uses." ('193 167:45-48) - 4. "to securely control access and other use, including distribution of records, documents, and notes associated with the case." ('193 274:34-36) - "Thus wrapped, a VDE object may be distributed to the recipient without fear of unauthorized access and/or other use. The one or more authorized users who have received an object are the only parties who may open that object and view and/or manipulate and/or otherwise modify its contents and VDE secure auditing ensures a record of all such user content activities." ('193 277:15-21) - "These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc." ('193 9:24-27) - "VDE provides a secure, distributed electronic transaction management system for controlling the distribution and/or other usage of electronically provided and/or stored information." ('193 9:36-39) - "As a result, VDE supports most types of electronic information and/or appliance: usage control (including distribution), security, usage auditing, reporting, other administration, and payment arrangements." ('193 13:50-53) - Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving.

Claim Term	MS Construction
	- Content (executables for example) delivered with proof of delivery and/or execution or other use. - "In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:24-31) - "Some or all of the back up files may be packaged within an administrative object and transmitted for analysis, transportation, or other uses." ('193 6:24-) - "Thus wrapped, a VDE object may be distributed to the recipient without fear of unauthorized access and/or other use. The one or more authorized users who have received an object are the only parties who may open that object and view and/or manipulate and/or otherwise modify its contents and VDE secure auditing ensures a record of all such user content activities." ('193 277:15-21) - "These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc". ('193 9:24-27) - "VDE provides a secure, distributed electronic transaction management system for controlling the distribution and/or other usage of electronically provided and/or stored information." ('193 9:36-39) - "As a result, VDE supports most types of electronic information and/or appliance: usage control (including distribution), security, usage auditing, reporting, other administration, and payment arrangements." ('193 13:50-53) - "SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected. ('193 59:48-59) - "Once the information is downloaded, the now-initialized PPE 650 can discard (or simply not use) the manufacturing key." ('193 212:57-59) Extrinsic: User: A person using a InterTrust node to perform some function (i.e., acting in some role). A user is identified with respect to the node by a user ID. (ITG, 5/12/95, IT00028300) User ID: Locally to a InterTrust node, each InterTrust user has an ID associated with a user name and authentication (e.g., password). In some deployments, there may be only one user, and access to the machine may be considered sufficient authentication; in such cases, the user ID concept may not be visible to the user even though it is present in the implementation. (ITG, 5/12/95, IT00028301) Use: To use an object is to access the content. This involves the processes of controlling and metering the use of the property and creating audit trail records on the use. (VDE ROI DEVICE v1.0a 9 Feb 1994, IT00008570)
user controls 683.2	Intrinsic: - "PPE 650 may perform various tests on the inputted item and/or other results of the user interaction provided by block 4512E in accordance with one or more user controls." ('683 39:19-21) ('193 26:39-67) "support user interaction through: ... (c) VDE aware applications which, as a result of the use of a VDE API and/or a transaction management (for example, ROS based) programming language embeds VDE "awareness" into commercial or internal software (application programs, games, etc.) so that VDE user control information and services are seamlessly integrated into such software .... For example, in a VDE aware word processor application, a user may be able to "print" a document into a VDE content container object, applying specific control information by selecting from amongst a series of different

Claim Term	MS Construction
	menu templates for different purposes (for example, a confidential memo template for internal organization purposes may restrict the ability to "keep," that is to make an electronic copy of the memo)." ('193 26:39) Extrinsic: Control: A business rule that governs the use of content. (ITG, 1997-1998, ML00012B) Control: A set of rules and consequences that apply to a governed element. The term control can apply to either a control program or a control set. (ITG, 1997-2000, ML00012D) Control: **Control Element*: A data structure that giverns (*sic)* the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). **Control mechanism*: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. **Control Parameter:* A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself. (ITG, 3/7/1995, IT00709618, see footnote 2) Control: Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node.(ITG, 5/12/95, IT00028293) Control: A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc. (ITG, 8/21/95, IT00032373, TD00068B) User: A person using a InterTrust node to perform some function (i.e., acting in some role). A user is identified with respect to the node by a user ID. (ITG, 5/12/95, IT00028300) User ID: Locally to a InterTrust node, each InterTrust user has an ID associated with a user name and authentication (e.g., password). In some deployments, there may be only one user, and access to the machine may be considered sufficient authentication; in such cases, the user ID concept may not be visible to the user even though it is present in the implementation. (ITG, 5/12/95, IT00028301) Extrinsic: User: 1. A person who requires the services of a computing system. 2. Any person or any thing that may issue or receive commands and messages to or from the information processing system. (IBM) User: 1. In communications security, any person who interacts directly with a network system. 4. In computer security, people who can access an AIS either by direct connections or indirect connections. (Longley) Control: The determination of the time and order in which the parts of a data processing system and the devices that contain those parts perform the input, processing, storage, and output functions.(IBM)
validity 912.8	Intrinsic: - "One of the functions SPU 500 may perform is to validate/authenticate VDE objects 300 and other items. Validation/authentication often involves comparing long data strings to determine whether they compare in a predetermined way." ('193 67:56-60) - ('193 73:24-25); ('193 73:26); ('193 78:6-17); ('193 87:47-55); ('193 112:46-61); ('193 210:28-35) Extrinsic: Validation: 1. In Cryptography, the process of checking the data integrity of a message, or selected parts of a message. (Longley) Validity Check: The process of analyzing data to determine whether it conforms to predetermined

Claim Term	MS Construction
	completeness and consistency parameters. (Microsoft Computer Dictionary, 3rd ed. 1997) "Validate – resolve references to other objects, check 'parameters'" (IT00051955)
Virtual distribution environment 900.155	Intrinsic: '193 203:58-67; '193 2:22 through conclusion of Background and Summary "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See 900.155 for Prosecution History limitations. "With respect to the remaining issues, Applicants respectfully disagree. For example, the Examiner objects to the use of "environment" as indefinite and unclear. This word, however, is not used in isolation, but rather in the context of several longer phrases, all of which are defined in the specification.. The phrase "protected processing environment," for example, is used in Claims 11 and 15-18 and described on at least, for example, pages 7-8 and 25 of the specification. The term "virtual distribution environment" used in Claim 11 is described, for example, on page 7 of the specification. The terms are also described in the commonly copending application Serial Number 08/388,107 of Ginter et al., filed 13 February 1995, entitled "System and Methods for Secure Transaction Management and Electronic Rights Protection." A copy of the incorporated Ginter application can be provided to the Examiner upon request." (pg. 13-14) (pages 7, 7-8 and 25 of the original specification are '721 2:62-3:13, 2:62-3:34 and 8:6-28 of the issued patent) 08/689,754 ('721), Amendment, 04/14/99, p. 13 - VDE supports a model wide, distributed security implementation which creates a single secure "virtual" transaction processing and information storage environment. VDE enables distributed VDE installations to securely store and communicate information and remotely control the execution processes and the character of use of electronic information at other VDE installations and in a wide variety of ways; ('193 21:57-65) - The rights protection problems solved by the present invention are electronic versions of basic societal issues. These issues include protecting property rights, protecting privacy rights, properly compensating people and organizations for their work and risk, protecting money and credit, and generally protecting the security of information. ('193 4:8-13) - The present invention provides a new kind of "virtual distribution environment" (called "VDE" in this document) that secures, administers, and audits electronic information use. ('193 2:24-27) - A fundamental problem for electronic content providers is extending their ability to control the use of proprietary information. Content providers often need to limit use to authorized activities and amounts. Participants in a business model involving, for example, provision of movies and advertising on optical discs may include actors, directors, script and other writers, musicians, studios, publishers, distributors, retailers, advertisers, credit card services, and content end-users. These participants need the ability to embody their range of agreements and requirements, including use limitations, into an "extended" agreement comprising an overall electronic business model. This extended agreement is represented by electronic content control information that can automatically enforce agreed upon rights and obligations. Under VDE, such an extended agreement may comprise an electronic contract involving all business model participants. Such an agreement may alternatively, or in addition, be made up of electronic agreements between subsets of the business model participants. Through the use of VDE, electronic commerce can function in the same way as traditional commerce-that is commercial relationships regarding products and services can be shaped through the negotiation of one or more agreements between a variety of parties. ('193 2:37-60) - "Protecting the rights of electronic community members involves a broad range of technologies. VDE combines these technologies in a way that creates a "distributed" electronic rights protection

Claim Term	MS Construction
	"environment." This environment secures and protects transactions and other processes important for rights protection. VDE, for example, provides the ability to prevent, or impede, interference with and/or observation of, important rights related transactions and processes." ('193 3:63-4:3) - "VDE is a cost-effective and efficient rights protection solution that provides a unified, consistent system for securing and managing transaction processing. VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:48-55) - In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed. ('193 6:24-30) - "A variety of capabilities are required to implement an electronic commerce environment. VDE is the first system that provides many of these capabilities and therefore solves fundamental problems related to electronic dissemination of information." ('193 8:16-20) - VDE offers an architecture that avoids reflecting specific distribution biases, administrative and control perspectives, and content types. Instead, VDE provides a broad-spectrum, fundamentally configurable and portable, electronic transaction control, distributing, usage, auditing, reporting, and payment operating environment. VDE is not limited to being an application or application specific toolset that covers only a limited subset of electronic interaction activities and participants. Rather, VDE supports systems by which such applications can be created, modified, and/or reused. As a result, the present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components. VDE can support a single electronic "world" within which most forms of electronic transaction activities can be managed. ('193 8:53-9:5) - "VDE can securely manage the integration of control information provided by two or more parties. As a result, VDE can construct an electronic agreement between VDE participants that represent a "negotiation" between, the control requirements of, two or more parties and enacts terms and conditions of a resulting agreement. VDE ensures the rights of each party to an electronic agreement regarding a wide range of electronic activities related to electronic information and/or appliance usage." ('193 9:52-61) - ""Hardware" 506 also contains long-term and short-term memories to store information securely so it can't be tampered with." ('193 60:1-3) - VDE prevents many forms of unauthorized use of electronic information, by controlling and auditing (and other administration of use) electronically stored and/or disseminated information. ('193 11:60-63) - Together, these VDE components comprise a secure, virtual, distributed content and/or appliance control, auditing (and other administration), reporting, and payment environment. ('193 13:14-17) - VDE can securely deliver information from one party to another concerning the use of commercially distributed electronic content. Even if parties are separated by several "steps" in a chain (pathway) of handling for such content usage information, such information is protected by VDE through encryption and/or other secure processing. Because of that protection, the accuracy of such information is guaranteed by VDE, and the information can be trusted by all parties to whom it is delivered. ('193 14:31-39) - VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a "virtual black box," a collection of distributed, very

Claim Term	MS Construction
	secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. ('193 15:14-27) - VDE provides organization, community, and/or universe wide secure environments whose integrity is assured by processes securely controlled in VDE participant user installations (nodes). ('193 20:48-51) - - "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... "employ "templates" to ease the process of configuring capabilities of the present invention as they relate to specific industries or businesses. ...Given the very large range of capabilities and configurations supported by the present invention, reducing the range of configuration opportunities to a manageable subset particularly appropriate for a given business model allows the full configurable power of the present invention to be easily employed by "typical" users who would be otherwise burdened with complex programming and/or configuration design responsibilities template applications can also help ensure that VDE related processes are secure and optimally bug free by reducing the risks associated with the contribution of independently developed load modules, including unpredictable aspects of code interaction between independent modules and applications, as well as security risks associated with possible presence of viruses in such modules. ... As the context surrounding these templates changes or evolves, template applications provided under the present invention may be modified to meet these changes for broad use, or for more focused activities. ... Of course, templates may, under certain circumstances have fixed control information and not provide for user selections or parameter data entry." ('193 21:43-53 27:1-28:18) - "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... provide mechanisms to persistently maintain trusted content usage and reporting control information through both a sufficiently secure chain of handling of content and content control information and through various forms of usage of such content wherein said persistence of control may survive such use. Persistence of control includes the ability to extract information from a VDE container object by creating a new container whose contents are at least in part secured and that contains both the extracted content and at least a portion of the control information which control information of the original container and/or are at least in part produced by control information of the original container for this purpose and/or VDE installation control information stipulates should persist and/or control usage of content in the newly formed container. Such control information can continue to manage usage of container content if the container is "embedded" into another VDE managed object, such as an object which contains plural embedded VDE containers, each of which contains content derived (extracted) from a different source." ('193 21:43-53 28:45-65) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... Interoperability is fundamental to efficient electronic commerce. The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad range of electronic appliances. ('193 21:43-45 34:25-30) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... securely support electronic currency and credit usage control, storage, and communication at, and between, VDE installations. ('193 21:43-45 36:49-51) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... requiring reporting and payment compliance by employing exhaustion of budgets and time ageing of keys. ('193 21:43-45 40:8-9) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... Because of the VDE security, including use of effective encryption, authentication, digital signaturing,

Claim Term	MS Construction
	and secure database structures, the records contained within a VDE card arrangement may be accepted as valid transaction records for government and/or corporate recordkeeping requirements. ('193 21:43-45 41:37-42) - Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed from outside observation and interference, the present invention ensures that content control information can be enforced. ('193 46:4-8) - An important feature of VDE is that it can be used to assure the administration of, and adequacy of security and rights protection for, electronic agreements implemented through the use of the present invention. ('193 46:51-54) - These are merely a few simple examples demonstrating the importance of ROS 602 ensuring that certain component assemblies 690 are formed in a secure manner. ROS 602 provides a wide range of protections against a wide range of "threats" to the secure handling and execution of component assemblies 690. ('193 85:15-20) - VDE further enables this process by providing a secure execution space in which the negotiation process(es) are assured of integrity and confidentiality in their operation. ('193 245:20-22) - "Taken together, and employed at times with VDE administrative objects and VDE security arrangements and processes, the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment." ('193 261:10-15) - For example, VDE 100 positively controls content access and usage, provides guarantee of payment for content used, and enforces budget limits for accessed content. ('193 240:53-56) - Such metering is a flexible basis for ensuring payment for content royalties, licensing, purchasing, and/or advertising. ('193 33:56-58) - The overall integrity and security of VDE 100 could ensure, in a coherent and centralized manner, that electronic reporting of tax related information (derived from one or more electronic commerce activities) would be valid and comprehensive. ('193 237:47-51) - Distributors 106 and financial clearinghouses 116 may themselves be audited based on secure records of their administrative activities and a chain of reliable, "trusted" processes ensures the integrity of the overall digital distribution process. This allows content owners, for example, to verify that they are receiving appropriate compensation based on actual content usage or other agreed-upon bases. ('193 254:66-255:5) - Because the control information is carried with each copy of a VDE protected document, and can ensure that central registries are updated and/or that originators are notified of document use, tracking can be prompt and accurate. ('193 281:14-16) - A final desirable feature of agreements in general (and electronic representations of agreements in particular) is that they be accurately recorded in a non-repudiatable form. In traditional terms, this involves creating a paper document (a contract) that describes the rights, restrictions, and obligations of all parties involved. This document is read and then signed by all parties as being an accurate representation of the agreement. Electronic agreements, by their nature, may not be initially rendered in paper. VDE enables such agreements to be accurately electronically described and then electronically signed to prevent repudiation. ('193 245:25-35) - As discussed above, a wide variety of techniques are currently being used to provide secure, trusted confidential delivery of documents and other items. Unfortunately, none of these previously existing mechanisms provide truly trusted, virtually instantaneous delivery on a cost-effective, convenient basis and none provide rights management and auditing through persistent, secure, digital information protection. In contrast, the present inventions provide the trustedness, confidentiality and security of a personal trusted courier on a virtually instantaneous and highly cost-effective basis. They provide techniques, systems and methods that can being to any form of electronic communications (including, but not

Claim Term	MS Construction
	limited to Internet and internal company electronic mail) an extremely high degree of trustedness, confidence and security approaching or exceeding that provided by a trusted personal courier. They also provide a wide variety of benefits that flow from rights management and secure chain of handling and control. ('683 5:20) - The Virtual Distribution Environment provides comprehensive overall systems, and wide arrays of methods, techniques, structures and arrangements, that enable secure, efficient electronic commerce and rights management on the Internet and other information superhighways and on internal corporate networks such as "Intranets". ('683 5:41) - "parties using the Virtual Distribution Environment can participate in commerce and other transactions in accordance with a persistent set of rules they electronically define." ('683 6:11) - "All of these various coordination steps can be performed nearly simultaneously, efficiently, rapidly and with an extremely high degree of trustedness based on the user of electronic containers 302 and the secure communications, authentication, notarization and archiving techniques provided in accordance with the present inventions." ('683 55:54) - "People are increasingly using secure digital containers to safely and securely store and transport digital content. One secure digital container model is the "DigiBox.TM." container developed by InterTrust Technologies, Inc. of Sunnyvale, Calif. The Ginter et al. patent specification referenced above describes many characteristics of this DigiBox.TM. container model—a powerful, flexible, general construct that enables protected, efficient and interoperable electronic description and regulation of electronic commerce relationship of all kinds, including the secure transport, storage and rights management interface with objects and digital information within such containers." ('861 1:35) - "Briefly, DigiBox containers are tamper-resistant digital containers that can be used to package any kind of digital information such as, for example, text, graphics, executable software, audio and/or video. The rights management environment in which DigiBox.TM. containers are used allows commerce participants to associate rules with the digital information (content). The rights management environment also allows rules (herein including rules and parameter data controls) to be securely associated with other rights management information, such as for example, rules, audit records created during use of digital information and administrative information associated with keeping the environment working properly, including ensuring rights and any agreements among parties. The DigiBox.TM.. electronic container can be used to store, transport and provide a rights management interfaces to digital information, related rules and other rights management information, as well as to other objects and/or data within a distributed, rights management environment. This arrangement can be used to provide electronically enforced chain of handling and control wherein rights management persists as a container moves from one entity to another. This capability helps support a digital rights management architecture that allows content rightsholders (including any parties who have system authorized interests related to such content, such as content republishes or even governmental authorities) to securely control and manage content, events, transactions, rules and usage consequences, including any required payment and/or usage reporting. This secure control and management continues persistently, protecting rights as content is delivered to, used by, and passed among creators, distributors, repurposes, consumers, payment disagregators, and other value chain participants... " ('861 1:47) - "Use of a secure electronic container containers to transport items providers an unprecedented degree of security, trustedness and flexibility." ('683 8:50) - "Virtual distribution environment 100 is "virtual" because it does not require many of the physical "things" that used to be necessary to protect rights, ensure reliable and predictable distribution, and ensure proper compensation to content creators and distributors." ('193 53:23-27) - VDE allows the needs of electronic commerce participants, to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present all physical locations where VDE related contents is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing

Claim Term	MS Construction
	functions (including metering) that operate within a "virtual black box"" a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means. ('193 15:14-27) - "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention ...VDE employs special purpose hardware distributed throughout some or all locations of a VDE implementation: a) said hardware controlling important elements of: content preparation (such as causing such content to be placed in a VDE content container and associating content control information with said content), content and/or electronic appliance usage auditing, content usage analysis, as well as content usage control; and b) said hardware having been designed to securely handle processing load module control activities, wherein said control processing activities may involve a sequence of required control factors" ('193 21:43-45 22:20-31) - Physical facility and user identity authentication security procedures may be used instead of hardware SPUs at certain nodes, such as at an established financial clearinghouse, where such procedures may provide sufficient security for trusted interoperability with a VDE arrangement employing hardware SPUs at user nodes. ('193 45:60-65) - An important part of VDE provided by the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other electronic appliance, or network. SPUs provide a trusted environment for generating decryption keys, encrypting and decrypting information, managing the secure communication of keys and other information between electronic appliances (i.e. between VDE installations and/or between plural VDE instances within a single VDE installation), securely accumulating and managing audit trail, reporting, and budget information in secure and/or non-secure non-volatile memory, maintaining a secure database of control information management instructions, and providing a secure environment for performing certain other control and administrative functions. ('193 48:66-49:14) - A hardware SPU (rather than a software emulation) within a VDE node is necessary if a highly trusted environment for performing certain VDE activities is required. ('193 49:15-17) - ""Hardware" 506 also contains long-term and short-term memories to store information securely so it can't be tampered with." ('193 60:1-3) - A VDE node's hardware SPU is a core component of a VDE secure subsystem and may employ some or all of an electronic appliance's primary control logic, such as a microcontroller, microcomputer or other CPU arrangement. This primary control logic may be otherwise employed for non VDE purposes such as the control of some or all of an electronic appliance's non-VDE functions. When operating in a hardware SPU mode, said primary control logic must be sufficiently secure so as to protect and conceal important VDE processes. For example, a hardware SPU may employ a host electronic appliance microcomputer operating in protected mode while performing VDE related activities, thus allowing portions of VDE processes to execute with a certain degree of security. ('193 49:33-46) - As shown FIG. 6, in the preferred embodiment, an SPU 500 may be implemented as a single integrated circuit "chip" 505 to provide a secure processing environment in which confidential and/or commercially valuable information can be safely processed, encrypted and/or decrypted. ('193 63:48-52) "SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 form being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected." ('193 59:48-59) - "SPU 500 may be surrounded by a tamper-resistant hardware security barrier 502. Part of this security barrier 502 is formed by a plastic or other package in which an SPU "die" is encased. Because the processing occurring within, and information stored by, SPU 500 are not easily accessible to the

Claim Term	MS Construction
	outside world, they are relatively secure from unauthorized access and tampering. All signals cross barrier 502 through a secure, controlled path provided by BIU 530 that restricts the outside world's access to the internal components within SPU 500. The secure, controlled path resists attempts form the outside world to access secret information and resources within SPU 500." ('193 63:60-64:5) - Regulation is ensured by control information put in place by one or more parties. ('193 6:34-35) -"Limited only by the VDE control information employed by content creators, other providers, and other pathway of handling and control participants, VDE allows a "natural" and unhindered flow of, and creation of, electronic content product models." ('193 297:25-29) - As a result, the present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components. ('193 8:62-9:3) - Independently, securely deliverable, component based control information allows efficient interaction among control information sets supplied by different parties. ('193 10:46-48) - A significant facet of the present invention's ability to broadly support electronic commerce is its ability to securely manage independently delivered VDE component objects containing control information (normally in the form of VDE objects containing one or more methods, data, or load module VDE components). This independently delivered control information can be integrated with senior and other pre-existing content control information to securely form derived control information using the negotiation mechanisms of the present invention. All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used. This means that, for example, all load modules and any mediating data which are listed by the derived control information as required must be available and securely perform their required function. ('193 10:66-11:14) - Content control information governs content usage according to criteria set by holders of rights to an object's contents and/or according to parties who otherwise have rights associated with distributing such content (such as governments, financial credit providers, and users). ('193 15:46-50) - In part, security is enhanced by object methods employed by the present invention because the encryption schemes used to protect an object can efficiently be further used to protect the associated content control information (software control information and relevant data) from modification. ('193 15:51-55) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... Content users, such as end-user customers using commercially distributed content (games, information resources, software programs, etc.), can define, if allowed by senior control information, budgets, and/or other control information, to manage their own internal use of content. ('193 21:43-45 29:3-8) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... support the separation of fundamental transaction control processes through the use of event (triggered) based method control mechanisms. These event methods trigger one or more other VDE methods (which are available to a secure VDE sub-system) and are used to carry out VDE managed transaction related processing. These triggered methods include independently (separably) and securely processable component billing management methods, budgeting management methods, metering management methods, and related auditing management processes. As a result of this feature of the present invention, independent triggering of metering, auditing, billing, and budgeting methods, the present invention is able to efficiently, concurrently support multiple financial currencies (e.g. dollars, marks, yen) and content related budgets, and/or billing increments as well as very flexible content distribution models. ('193 21:43-45 42:21-38) - support, complete, modular separation of the control structures related to (1) content event triggering, (2) auditing, (3) budgeting (including specifying no right of use or unlimited right of use), (4) billing, and (5) user identity (VDE installation, client name, department, network, and/or user, etc.). The

Claim Term	MS Construction
	independence of these VDE control structures provides a flexible system which allows plural relationships between two or more of these structures, for example, the ability to associate a financial budget with different event trigger structures (that are put in place to enable controlling content based on its logical portions). Without such separation between these basic VDE capabilities, it would be more difficult to efficiently maintain separate metering, budgeting, identification, and/or billing activities which involve the same, differing (including overlapping), or entirely different, portions of content for metering, billing, budgeting, and user identification, for example, paying fees associated with usage of content, performing home banking, managing advertising services, etc. VDE modular separation of these basic capabilities supports the programming of plural, "arbitrary" relationships between one or differing content portions (and/or portion units) and budgeting, auditing, and/or billing control information. ('193 42:39-63) - The virtual distribution environment 100 prevents use of protected information except as permitted by the "rules and controls" (control information). For example, the "rules and controls" shown in FIG. 2 may grant specific individuals or classes of content users 112 "permission" to use certain content. They may specify what kinds of content usage are permitted, and what kinds are not. They may specify how content usage is to be paid for and how much it costs. As another example, "rules and controls" may require content usage information to be reported back to the distributor 106 and/or content creator 102. ('193 56:26-35) - "ROS VDE functions 604 may be based on segmented, independently loadable executable "component assemblies" 690. These component assemblies 690 are independently securely deliverable. The component assemblies 690 provided by the preferred embodiment comprise code and data elements that are themselves independently deliverable.... These component assemblies 690 are the basic functional unit provided by ROS 602. The component assemblies 690 are executed to perform operating system or application tasks. Thus, some component assemblies 690 may be considered to be part of the ROS operating system 602, while other component assemblies may be considered to be "applications" that run under the support of the operating system." ('193 83:12-29) - "As mentioned above, ROS 602 provides several layers of security to ensure the security of component assemblies 690. One important security layer involves ensuring that certain component assemblies 690 are formed, loaded and executed only in secure execution space such as provided within an SPU 500." ('193 87:33-38) - "Methods 1000 perform the basic function of defining what users (including, where appropriate, distributions, client administration, etc.), can and cannot do with an object 300." ('193 128:30-33) - "Container 152 in this example further includes an electronic control set 188 describing conditions under which the power may be exercised. Controls 188 define the power(s) granted to each of the participants – including (in this example) conditions or limitations for exercising these powers. Controls 188 may provide the same powers and/or conditions of use for each participant, or they may provide different powers and/or conditions of use for each participant." ('712 220: 1-8) - "...content creators and rights owners can register permissions with the rights and permissions clearinghouses 400 in the form of electronic "control sets." These permissions can specify what consumers can and can't do with digital properties, under what conditions the permissions can be exercised and the consequences of exercising the permissions." ('712 72:2-7) - "This "channel 0" "open channel" task may then issue a series of requests to secure database manager 566 to obtain the "blueprint" for constructing one or more component assemblies 690 to be associated with channel 594 (block 1127). In the preferred embodiment, this "blueprint" may comprise a PERC 808 and/or URT 464." ('193 112:46-51) - In part, security is enhanced by object methods employed by the present invention because the encryption schemes used to protect an object can efficiently be further used to protect the associated content control information (software control information and relevant data) from modification. ('193 15:51-55) - FIG. 5A shows how the virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a "container" 302 so the information can't be accessed

Claim Term	MS Construction
	except as provided by its "rules and controls." Normally, the container 302 is electronic rather than physical. Electronic container 302 in one example comprises "digital" information having a well defined structure. Container 302 and its contents can be called an "object 300." ('193 58:39-46) - "Moreover, when any new VDE object 300 arrives at an electronic appliance 600, the electronic appliance must "register" the object within object registry 450 so that it can be accessed." ('193 153:56-59) - "Even if the object is stored locally to the VDE node, it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object." ('193 192:14-19) - "ACCESS method 2000 reads the ACCESS method MDE from the secure database, reads it in accordance with the ACCESS method DTD, and loads encrypted content source and routing information based on the MDE (blocks 2010, 2012). This source and routing information specifies the location of the encrypted content. ACCESS method 2000 then determines whether a connection to the content is available (decision block 2014). This "connection" could be, for example, an on-line connection to a remote site, a real-time information feed, or a path to a secure/protected resource, for example. If the connection to the content is not currently available ("No" exit of decision block 2014), then ACCESS method 2000 takes steps to open the connection (block 2016). If the connection fails (e.g., because the user is not authorized to access a protected secure resource), then the ACCESS method 2000 returns with a failure indication (termination point 2018)." ('193 192:36-52) - "It also employs a software object architecture for VDE content containers that carries protected content and may also carry both freely available information (e.g., summary, table of contents) and secured content control information which ensures the performance of control information." ('193 15:41-46) - "In this example, creator 102 may employ one or more application software programs and one or more VDE secure subsystems to place unencrypted content into VDE protected form (i.e., into one or more VDE content containers)." ('193 315:53-56) - "The Ginter et al. patent specification referenced above describes many characteristics of this DigiBox™ container model, a powerful, flexible, general construct that enables protected, efficient and interoperable electronic description and regulation of electronic commerce relationships of all kinds..." ('861 1:39)] - "The node and container model described above and in the Ginter et al. patent specification (along with similar other DigiBox/VDE (Virtual Distribution Environment) models) has nearly limitless flexibility." ('861 2:37) - Therefore, the container creation and usage tools must themselves be secure in the sense that they must protect certain details about the container design. This additional security requirement can make it even more difficult to make containers easy to use and to provide interoperability. ('861 4:59) - "FIG. 88 illustrates secure electronic container 302 as an attaché handcuffed to the secure delivery person's wrist. Once again, container is shown as a physical thing for purposes of illustrations only –in the example it is preferably electronic rather than physical, and comprises digital information having a well-defined structure (see FIG. 5A). Special mathematical techniques known as "cryptography" can be used to make electronic container 302 secure so that only intended recipient 4056 can open the container and access the electronic document (or other items) 4054 it contains." ('683 15:61) - "Appliance 600B may deliver the digital copy of item 4054 within container 302 and/or protect the item with seals. Electronic fingerprints, watermarks and/.or other visible and/or hidden markings to provide a "virtual container or some of the security or other characteristics of a container (for example, the ability to associate electronic controls with the item). ('683 18:) - "For example, defendant's attorney 5052 can specify one container 302 for opening by his co-counsel, client or client in-house counsel, and program another container 302 for opening only by opposing (plaintiff's) counsel 5050. Because of the unique trustedness features provided by system 4050, the defendant's attorney 5052 can have a high degree of trust and confidence that only the

Claim Term	MS Construction
	authorized parties will be able to open the respective containers and access the information they contain." ('683 56:17) - "The "container" concept is a convenient metaphor used to give a name to the collection of elements *required to make use of content* or to perform an administrative-type activity." ('193 127:30-32) - "the virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a "container" 302 so the information can't be accessed except as provided by its "rules and controls."" ('193 58:39-43) - "VDE 100 provides a media independent container model for encapsulating content." ('193 127:2-3) - "The electronic form of a document is stored as a VDE container (object) associated with the specific client and/or case. The VDE container mechanism supports a hierarchical ordering scheme for organizing files and other information with a container; this mechanism may be used to organize the electronic copies of the documents within a container, A VDE container is associated with specific access control information and rights that are described in one or more permissions control information sets (PERCs) associated with that container. In this example, only those members of the law firm who possess a VDE instance, an appropriate PERC, and the VDE object that contains the desired document, may use the document." ('193 274:52-64) - "The situation is no better for processing documents within the context of ordinary computer and network systems. Although said systems can enforce access control information based on user identity, and can provide auditing mechanism for tracking accesses to files, these are low-level mechanisms that do not permit tracking or controlling the flow of content. In such systems, because document content can be freely copied and manipulated, it is not possible to determine where documents content has gone, or where it came from." ('193 281:27-35) - "Secure containers 302 may be used to encapsulate the video and audio being exchanged between electronic kiosk appliances 600, 600' to maintain confidentiality and ensure a high degree of trustedness. - "Because container 152 can only be opened within a secure protected processing environment 154 that is part of the virtual distribution environment described in the above-referenced Ginter et al. patent disclosure" - "The present invention provides a new kind of "virtual distribution environment" (called "VDE" in this document) that secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for ...." ('193 2:24-28) -"the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment." ('193 261:12-15) -"The inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention. Despite the attention devoted by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems." ('193 2:13-22) -"The configurability provided by the present invention is particularly critical for supporting electronic commerce, that is enabling businesses to create relationships and evolve strategies that offer competitive value. Electronic commerce tools that are not inherently configurable and interoperable will ultimately fail to produce products (and services) that meet both basic requirements and evolving needs of most commerce applications." ('193 16:41-48) -"VDE also extends usage control information to an arbitrary granular level (as opposed to a file based level provided by traditional operating systems) and ...." ('193 275:8-11) -Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: ...." ('193 21:43-45) -"A significant facet of the present invention's ability to broadly support electronic commerce is its

Claim Term	MS Construction
	ability to securely manage independently delivered VDE component objects containing control information ...." ('193 10:66-11:2) -"Some of the key factors contributing to the configurability intrinsic to the present invention include: ...." ('193 16:66-67) -"The scalable transaction management/auditing technology of the present invention will result in more efficient and reliable interoperability ...." ('193 34:9-11) -"the present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components." ('193 8:63-9:3) -"The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad range of electronic appliances." ('193 34:26-30) -"The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable." ('193 128:28-30) -"An important feature of VDE is that it can be used to assure the administration of, and adequacy of security and rights protection for, electronic agreements implemented through the use of the present invention." ('712 168:22-25) -"In this example, both the address request 602 and the responsive information 604 are contained within secure electronic containers 152 in order to maintain the confidentiality and integrity of the requests and responses. In this way, for example, outside eavesdroppers cannot tell who sender 95(1) wants to communicate with or what information he or she needs to perform communications with or what information he or she needs to perform the communications – and the directory responses cannot be "spoofed" to direct the requested message to another location." ('712 12:15-22) Components: "On the other hand, if the information to be exchanged has already been secured and/or is available without authentication (e.g., certain catalog information, containers that have already been encrypted and do not require special handling, etc.), the "weaker" for of login/password may be used." ('193 290:57-62) Components: "VDE provides means to securely combine content provided at different times, by differing sources, and/or representing different content types. These types, timings, and/or different sources of content can be employed to form a complex array of content within a VDE content container objects, each containing different content whose usage can be controlled, at least in part, by its own container's set of VDE content control information." ('193 397:35-) Container-Related Methods: "Although methods 1000 can have virtually unlimited variety and some may even be user-defined, certain basic "use" type methods are preferably used in the preferred embodiment to control most of the more fundamental object manipulation and other functions provided by VDE 100. For example, the following high level methods would typically be provided for object manipulation; OPEN method, READ method, WRITE method, CLOSE method. An OPEN method is used to control opening a container so its content may be accessed. A READ method is used to control access to contents in a container. A WRITE method is used to control the insertion of contents into a container. A CLOSE method is used to close a container that has been opened." ('193 183:12-29)[5] - "DESTROY method 2180 removes the ability of a user to use an object by destroying the URT the user requires to access the object. In the preferred embodiment, ... DESTROY method 2180 may than call a WRITE and/or ACCESS method to write information which will corrupt (and thus destroy) the header and/or other important parts of the object (block 2186). DESTROY method 2180 may then mark one or more of the control structures (e.g., the URT) as damaged by writing appropriate information to control structure (blocks 2188, 2190)." ('193 198:41-45) - "PANIC method 2200 may prevent the user from further accessing the object currently being accessed

Claim Term	MS Construction
	by, for example, destroying the channel being used to access the object and marking one or more of the control structures (e.g., the URT) associated with the user and object as damaged.(blocks 2206, and 2208-2210, respectively). Because the control structure is damaged, the VDE node will need to contact an administrator to obtain a valid control structure(s) before the user may access the same object again." ('193 198:60-199:2) - "EXTRACT method 2080 is used to copy or remove content from an object and place it into a new object. In the preferred embodiment, the EXTRACT method 2080 does not involve any release of content, but rather simply takes content from one container and places it into another container, both of which may be secure. Extraction of content differs from release in that the content is never exposed outside a secure container." ('193 194:13-20) - "Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility." ('683 8:50) -"Electronic delivery person 4060 can deliver the electronic version of item 4054 within secure container attaché case 302 from personal computer 4116' to another personal computer 4116 operated by recipient 4056." ('683 20:27) - "Because these transactions are conducted using VDE and VDE secure containers, those observing the communications learn no more than the fact that the parties are communicating." ('712 310:1-3) - "VDE in one example provides a "virtual silicon container" ("virtual black box") in that several different instances of SPU 500 may securely communicate together to provide an overall secure hardware environment that "virtually" exists at multiple locations and multiple electronic appliances 600. FIG. 87 shows one model 3600 of a virtual silicon container. This virtual container model 3600 includes a content creator 102, a content distributor 106, one or more content redistributors 106a, one or more client administrators 700, one or more client users 3602, and one or more clearinghouses 116. Each of these various VDE participants has an electronic appliance 600 including a protected processing environment 655 that may comprise, at least in part, a silicon-based semiconductor hardware element secure processing unit 500. The various SOUs 500 each encapsulate a part of the virtual distribution environment, and thus, together form the virtual silicon container 3600." ('193 317:58-318:8) -"uses tools to transform digital information(such as electronic books, databases, computer software and movies) into protected digital packages called "objects." Only those consumers (or other along the chain of possession such as redistributor) who receive permission from a distributor 106 can open these packages. VDE packaged content can be constrained by "rules and control information."" ('193 254:18-25) -"To open VDE package and make use of its content, and end-user must have permission." ('193 254:45-46) - "place unencrypted content into VDE protected form (i.e., into one or more VDE content containers)." ('193 315:55-56) - "VDE can protect a collection of rights belonging to various parties having in rights in, or to, electronic information. This information may be at one location or dispersed across (and/or moving between) multiple locations. The information may pass through a "chain" of distributors and a "chain" of users. Usage information may also be reported through one or more "chains" of parties. In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:18-31) - All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used. ('193 11:8-11) - "VDE provides important mechanisms for both enforcing commercial agreements and enabling the protection of privacy rights. VDE can securely deliver information from one party to another

Claim Term	MS Construction
	concerning the use of commercially distributed electronic content. Even if parties are separated by several "steps" in a chain (pathway) of handling for such content usage information, such information is protected by VDE through encryption and/or other secure processing. Because of that protection, the accuracy of such information is guaranteed by VDE, and the information can be trusted by all parties to whom it is delivered." ('193 14:29-39) - VDE ensures that certain prerequisites necessary for a given transaction to occur are met. This includes the secure execution of any required load modules and the availability of any required, associated data. ('193 20:27-30) - Required methods (methods listed as required for property and/or appliance use) must be available as specified if VDE controlled content (such as intellectual property distributed within a VDE content container) is to be used. ('193 43:37-41) - "Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed from outside observation and interference, the present invention ensures that content control information can be enforced. ('193 46:4-8) - This control information can determine, for example: (1) How and/or to whom electronic content can be provided, for example, how an electronic property can be distributed; (2) How one or more objects and/or properties, or portions of an object or property, can be directly used, such as decrypted, displayed, printed, etc; .... ('193 46:17-24) ""Hardware" 506 also contains long-term and short-term memories to store information securely so it can't be tampered with." ('193 60:1-3) "A feature of VDE provided by the present invention is that certain one or more methods can be specified as required in order for a VDE installation and/or user to be able to use certain and/or all content. ('193 43:47-50) The virtual distribution environment 100 prevents use of protected information except as permitted by the "rules and controls" (control information). ('193 56:26-28) - As mentioned above, virtual distribution environment 100 "associates" content with corresponding "rules and controls," and prevents the content from being used or accessed unless a set of corresponding "rules and controls" is available. The distributor 106 doesn't need to deliver content to control the content's distribution. The preferred embodiment can securely protect content by protecting corresponding, usage enabling "rules and controls" against unauthorized distribution and use. ('193 57:18-26) - Since no one can use or access protected content without "permission" from corresponding "rules and controls," the distributor 106 can control use of content that has already been (or will in the future be) delivered. ('193 57:30-33) - SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. ('193 59:48-55) - Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, redistributing (including to what one or more parties), and/or saving. - In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed. ('193 6:24-30) - to securely control access and other use, including distribution of records, documents, and notes associated with the case, ('193 274:34-36)

Claim Term	MS Construction
	- Thus wrapped, a VDE object may be distributed to the recipient without fear of unauthorized access and/or other use. ('193 277:16-17) - These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc.('193 9:24-27) - VDE provides a secure, distributed electronic transaction management system for controlling the distribution and/or other usage of electronically provided and/or stored information. ('193 9:36-39) - "The doctor 5000 may then send container 301(1) to a trusted go-between 4700. ...For example, the trusted go-between 4700 in one example has no access to the content of the container 302(1), but does have a record of a seal of the contents." ('683 53:40) - "FIG. 116 shows example steps that may be performed by PPE 650 in response to an "open" or "view" event. In this example, PPE 650 may - - upon allowing recipient 4056 to actually interact with the item 4054--...PPE 650 may then release the image 4068I and/or the data 4068D to the application running on electronic appliance 600—electronic fingerprinting or watermarking the released content if appropriate (FIG. 116, block 4625C). ('683 42:38) - FIG. 5A shows how the virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a "container" 302 so the information can't be accessed except as provided by its "rules and controls." ('193 58:39-43) - Each VDE participant in a VDE pathway of content control information may set methods for some or all of the content in a VDE container, so long as such control information does not conflict with senior control information already in place with respect to: (1) certain or all VDE managed content, (2) certain one or more VDE users and/or groupings of users, (3) certain one or more VDE nodes and/or groupings of nodes, and/or (4) certain one or more VDE applications and/or arrangements. ('193 44:6-17) - "All participants of VDE 100 have the innate ability to participate in any role." ('193 256:50-51) - "Any VDE user 112 may assign the right to process information or perform services on their behalf to the extend allowed by senior control information." ('193 257:17-20) - "PERC and URT structures provide a mechanism that may be used to provide precise electronic representation of rights and the controls associated with those rights. VDE thus provides a "vocabulary" and mechanism by which users and creators may specify their desires." ('193 245:11-) - "VDE provides comprehensive and configurable transaction management, metering and monitoring technology." ('193 3:34) - VDE may be combined with, or integrated into, many separate computers and/or other electronic appliances. These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc. The secure subsystem in the preferred embodiment comprises one or more "protected processing environments", one or more secure databases, and secure "component assemblies" and other items and processes that need to be kept secured. VDE can, for example, securely control electronic currency, payments, and/or credit management (including electronic credit and/or currency receipt, disbursement, encumbering, and/or allocation) using such a "secure subsystem." ('193 9:22) - "In addition VDE: (a) is very configurable, modifiable, and re-usable; (b) supports a wide range of useful capabilities that may be combined in different ways to accommodate most potential applications; (c) operates on a wide variety of electronic appliances ranging from hand-held inexpensive devices to large mainframe computers;

Claim Term	MS Construction
	(d) is able to ensure the various rights of a number of different parties, and a number of different rights protection schemes, simultaneously; (e) is able to preserve the rights of parties through a series of transactions that may occur at different times and different locations; (f) is able to flexibly accommodate different ways of securely delivering information and reporting usage; and (g) provides for electronic analogues to "real" money and credit, including anonymous electronic cash, to pay for products and services and to support personal (including home) banking and other financial activities." ('193 4:57) - It can provide efficient, reusable, modifiable, and consistent means for secure electronic content: distribution, usage control, usage payment, usage auditing, and usage reporting. ('193 8:26) - VDE offers an architecture that avoids reflecting specific distribution biases, administrative and control perspectives, and content types. Instead, VDE provides a broad-spectrum, fundamentally configurable and portable, electronic transaction control, distributing, usage, auditing, reporting, and payment operating environment. ('193 8:53) - The present invention allows content providers and users to formulate their transaction environment to accommodate: (1) desired content models, content control models, and content usage information pathways, (2) a complete range of electronic media and distribution means, (3) a broad range of pricing, payment, and auditing strategies, (4) very flexible privacy and/or reporting models, (5) practical and effective security architectures, and (6) other administrative procedures that together with steps (1) through (5) can enable most "real world" electronic commerce and data security models, including models unique to the electronic world. ('193 10:11) - Because of the breadth of issues resolved by the present invention, it can provide the emerging "electronic highway" with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions. ('193 17:22) - "A feature of the present invention provides for payment means supporting flexible electronic currency and credit mechanisms, including the ability to securely maintain audit trails reflecting information related to use of such currency or credit.' ('193 33:58) - "the end-to-end nature of VDE applications, in which content 108 flows in one direction, generating reports and bills 118 in the other, makes it possible to perform "back-end" consistency checks." ('193 223:17) - By way of non-exhaustive summary, these present inventions provide a highly secure and trusted item delivery and agreement execution services providing the following features and functions: Trustedness and security approaching or exceeding that of a personal trusted courier. Instant or nearly instant delivery. Optional delayed delivery ("store and forward"). Broadcasting to multiple parties. Highly cost effective. Trusted validation of item contents and delivery. Value Added Delivery and other features selectable by the sender and/or recipient. Provides electronic transmission trusted auditing and validating. Allows people to communicate quickly, securely, and confidentially. Communications can later be proved through reliable evidence of the communications transaction--providing non-repudiatable, certain, admissible proof that a particular communications transaction occurred. Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving.

Claim Term	MS Construction
	Supports persistent rights and rules based document workflow management at recipient sites. System may operate on the Internet, on internal organization and/or corporate networks ("intranets" irrespective of whether they use or offer Internet services internally), private data networks and/or using any other form of electronic communications. System may operate in non-networked and/or intermittently networked environments. Legal contract execution can be performed in real time, with or without face to face or ear-to-ear personal interactions (such as audiovisual teleconferencing, automated electronic negotiations, or any combination of such interactions) for any number of distributed individuals and/or organizations using any mixture of interactions. The items delivered and/or processed may be any "object" in digital format, including, but not limited to, objects containing or representing data types such as text, images, video, linear motion pictures in digital format, sound recordings and other audio information, computer software, smart agents, multimedia, and/or objects any combination of two or more data types contained within or representing a single compound object. Content (executables for example) delivered with proof of delivery and/or execution or other use. Secure electronic containers can be delivered. The containers can maintain control, audit, receipt and other information and protection securely and persistently in association with one or more items. Trustedness provides non-repudiation for legal and other transactions. Can handle and send any digital information (for example, analog or digital information representing text, graphics, movies, animation, images, video, digital linear motion pictures, sound and sound recordings, still images, software computer programs or program fragments, executables, data, and including multiple, independent pieces of text; sound clips, software for interpreting and presenting other elements of content, and anything else that is electronically representable). Provides automatic electronic mechanisms that associate transactions automatically with other transactions. System can automatically insert or embed a variety of visible or invisible "signatures" such as images of handwritten signatures, seals, and electronic "fingerprints" indicating who has "touched" (used or other interacted with in any monitorable manner) the item. System can affix visible seals on printed items such as documents for use both in encoding receipt and other receipt and/or usage related information and for establishing a visible presence and impact regarding the authenticity, and ease of checking the authenticity, of the item. Seals can indicate who originated, sent, received, previously received and redistributed, electronically view, and/or printed and/or otherwise used the item. Seals can encode digital signatures and validation information providing time, location, send and/or other information and/or providing means for item authentication and integrity check. Scanning and decoding of item seals can provide authenticity/integrity check of entire item(s) or part of an item (e.g., based on number of words, format, layout, image--picture and/or test--composition, etc.). Seals can be used to automatically associate electronic control sets for use in further item handling. System can hide additional information within the item using "stenanography" for later retrieval and analysis. Steganography can be used to encode electronic fingerprints and/or other information into an item to prevent deletion. Multiple stenanographic storage of the same fingerprint information may be employed reflecting "more" public and "less" public modes so that a less restricted steganographic mode (different encryption algorithm, keys, and/or embedding techniques) can be used to assist easy recognition by an authorized party and a more private (confidential) mode may be readable by only a few parties (or only one party) and comprise of the less restricted mode may not affect the security of the more private mode. Items such as documents can be electronically, optically scanned at the sender's end--and printed out in original, printed form at the recipient's end. Document handlers and processors can integrate document scanning and delivery. Can be directly integrated into enterprise and Internet (and similar network) wide document workflow systems and applications. Secure, tamper-resistant electronic appliance, which may employ VDE SPUs, used to handle items at both sender and recipient ends.

Claim Term	MS Construction
	"Original" item(s) can automatically be destroyed at the sender's end and reconstituted at the recipient's end to prevent two originals from existing simultaneously. Secure, non-repudiable authentication of the identification of a recipient before delivery using any number of different authentication techniques including but not limited to biometric techniques (such as palm print scan, signature scan, voice scan, retina scan, iris scan, biometric fingerprint and/or handprint scan, and/or face profile) and/or presentation of a secure identity "token." Non-repudiation provided through secure authentication used to condition events (e.g., a signature is affixed onto a document only if the system securely authenticates the sender and her intention to agree to its contents). Variety of return receipt options including but not limited to a receipt indicating who opened a document, when, where, and the disposition of the document (stored, redistributed, copied, etc.). These receipts can later be used in legal proceedings and/or other contexts to prove item delivery, receipt and/or knowledge. Audit, receipt, and other information can be delivered independently from item delivery, and become securely associated with an item within a protected processing environment. Secure electronic controls can specify how an item is to be processed or otherwise handled (e.g., document can't be modified, can be distributed only to specified persons, collections of persons, organizations, can be edited only by certain persons and/or in certain manners, can only be viewed and will be "destroyed" after a certain elapse of time or real time or after a certain number of handlings, etc.) Persistent secure electronic controls can continue to supervise item workflow even after it has been received and "read." Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility. Secure controls can be used in conjunction with digital electronic certificates certifying as to identity, class (age, organization membership, jurisdiction, etc.) of the sender and/or receiver and/or user of communicated information. Efficiently handles payment and electronic addressing arrangements through use of support and administrative services such as a Distributed Commerce Utility as more fully described in the copending Shear, et al. application. Compatible with use of smart cards, including, for example, VDE enabled smart cards, for secure personal identification and/or for payment. Transactions may be one or more component transactions of any distributed chain of handling and control process including Electronic Data Interchange (EDI) system, electronic trading system, document workflow sequence, and banking and other financial communication sequences, etc. ('683 6:18) - "Content providers and distributors have devised a number of limited function rights protection mechanisms to protect their rights. Authorization passwords and protocols, license servers, "lock/unlock" distribution methods, and non-electronic contractual limitations imposed on users of shrink-wrapped software are a few of the more prevalent content protection schemes. In a commercial context, these efforts are inefficient and limited solutions." ('900 2:64) - "The inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention. Despite the attention devoted by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems." ('193 2:13) - "The features of VDE allow it to function as the first trusted electronic information control environment that can conform to, and support, the bulk of conventional electronic commerce and data security requirements. In particular, VDE enables the participants in a business value chain model to create an electronic version of traditional business agreement terms and conditions and further enables these participants to shape and evolve their electronic commerce models as they believe appropriate to their business requirements." ('193 8:43)

Claim Term	MS Construction
	- An objective of VDE is supporting a transaction/distribution control standard. Development of such a standard has many obstacles, given the security requirements and related hardware and communications issues, widely differing environments, information types, types of information usage, business and/or data security goals, varieties of participants, and properties of delivered information. A significant feature of VDE accommodates the many, varying distribution and other transaction variables by, in part, decomposing electronic commerce and data security functions into generalized capability modules executable within a secure hardware SPU and/or corresponding software subsystem and further allowing extensive flexibility in assembling, modifying, and/or replacing, such modules (e.g. load modules and/or methods) in applications run on a VDE installation foundation. This configurability and reconfigurability allows electronic commerce and data security participants to reflect their priorities and requirements through a process of iteratively shaping an evolving extended electronic agreement (electronic control model). ('193 15:66) - Some of the key factors contributing to the configurability intrinsic to the present invention include: (a) integration into the fundamental control environment of a broad range of electronic appliances through portable API and programming language tools that efficiently support merging of control and auditing capabilities in nearly any electronic appliance environment while maintaining overall system security; (b) modular data structures; (c) generic content model; (d) general modularity and independence of foundation architectural components; (e) modular security structures; (f) variable length and multiple branching chains of control; and (g) independent, modular control structures in the form of executable load modules that can be maintained in one or more libraries, and assembled into control methods and models, and where such model control schemes can "evolve" as control information passes through the VDE installations of participants of a pathway of VDE content control information handling. ('193 16:66) - "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... provide mechanisms that allow control information to "evolve" and be modified according, at least in part, to independently, securely delivered further control information. ... Handlers in a pathway of handling of content control information, to the extent each is authorized, can establish, modify, and/or contribute to, permission, auditing, payment, and reporting control information related to controlling, analyzing, paying for, and/or reporting usage of, electronic content and/or appliances (for example, as related to usage of VDE controlled property content)." ('193 21:43, 29:21) - "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... enable a user to securely extract, through the use of the secure subsystem at the user's VDE installation, at least a portion of the content included within a VDE content container to produce a new, secure object (content container), such that the extracted information is maintained in a continually secure manner through the extraction process." ('193 21:43 31:66) - "As with the content control information for most VDE managed content, features of the present invention allows [sic] the content's control information to: (a) "evolve," for example, the extractor of content may add new control methods and/or modify control parameter data, such as VDE application compliant methods, to the extent allowed by the content's in-place control information. ... (b) allow a user to combine additional content with at least a portion of said extracted content, ... (c) allow a user to securely edit at least a portion of said content while maintaining said content in a secure form within said VDE content container; ... (d) append extracted content to a pre-existing VDE content container object and attach associated control information ... (e) preserve VDE control over one or more portions

Claim Term	MS Construction
	of extracted content after various forms of usage of said portions ... Generally, the extraction features of the present invention allow users to aggregate and/or disseminate and/or otherwise use protected electronic content information extracted from content container sources while maintaining secure VDE capabilities thus preserving the rights of providers in said content information after various content usage processes." ('193 32:27) - The secure component based architecture of ROS 602 has important advantages. For example, it accommodates limited resource execution environments such as provided by a lower cost SPU 500. It also provides an extremely high level of configurability. In fact, ROS 602 will accommodate an almost unlimited diversity of content types, content provider objectives, transaction types and client requirements. In addition, the ability to dynamically assemble independently deliverable components at execution time based on particular objects and users provides a high degree of flexibility, ('193 87:63) - "Each logical object structure 800 may also include a "private body" 806 containing or referencing a set of methods 1000 (i.e., programs or procedures) that control use and distribution of the object 300. The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable." ('193 128:25) - "VDE methods 1000 are designed to provide a very flexible and highly modular approach to secure processing." ('193 181:17) - "The reusable functional primitives of VDE 100 can be flexibly combined by content providers to reflect their respective distribution objectives." ('193 255:27) - the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment." ('193 261:12) - "Adding new content to objects is an important aspect of authoring provided by the present invention. Providers may wish to allow one or more users to add, hide, modify, remove and/or extend content that they provide. In this way, other users may add value to, alter for a new purpose, maintain, and/or otherwise change, existing content. The ability to add content to an empty and/or newly created object is important as well." ('193 261:23) - "The distribution control information provided by the present invention allows flexible positive control. No provider is required to include any particular control, or use any particular strategy, except as required by senior control information. Rather, the present invention allows a provider to select from generic control components (which may be provided as a subset of components appropriate to a provider's specific market, for example, as included in and/or directly compatible with, a VDE application) to establish a structure appropriate for a given chain of handling/control." ('193 297:9)"Importantly, VDE securely and flexibly supports editing the content in, extracting content from, embedding content into, and otherwise shaping the content composition of, VDE content containers. Such capabilities allow VDE supported product models to evolve by progressively reflecting the requirements of "next" participants in an electronic commercial model." ('193 297:9) - "For instance, the user may have an "access" right, and an "extraction" right, but not a "copy" right." ('193 159:24) - "PERCS 808 specify a set of rights that may be exercised to use or access the corresponding VDE object 300. The preferred embodiment allows users to "customize" their access rights by selecting a subset of rights authorized by a corresponding PERC 808 and/or by specifying parameters or choices that correspond to some or all of the rights granted by PERC 808. These user choices are set forth in a user rights table 464 in the preferred embodiment. User rights table (URT) 464 includes URT records, each of which correspond to a user (or group of users). Each of these URT records specific users choices for a corresponding VDE object more methods 1000 for exercising the rights granted to the user by the PERC 808 in a way specified by the choices contained within the URT record." ('193 156:55) - "PERC and URT structures provide a mechanism that may be used to provide precise electronic representation of rights and the controls associated with those rights. VDE thus provides a

Claim Term	MS Construction
	"vocabulary" and mechanism by which users and creators may specify their desires." ('193 245:10) - "In sum, the present invention allows information contained in electronic information products to be supplied according to user specification. Tailoring to user specification allows the present invention to provide the greatest value to users, which in turn will generate the greatest amount of electronic commerce activity." ('193 22:66) - Function: "Adding new content to objects is an important aspect of authoring provided by the present invention. Providers may wish to allow one or more users to add, hide, modify, remove and/or extend content that they provide. In this way, other users may add value to, alter for a new purpose, maintain, and/otherwise change, existing content. The ability to add content to an empty and/or newly created object is important as well." ('193 261:23) - Function: "Each logical object structure 800 may also include a "private body" 806 containing or referencing a set of method 1000 (i.e., programs or procedures) that control use and distribution of the object 300. The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable." ('193 128:25) - Function: "An important aspect of adding or modifying content is the choice of encryption/decryption keys and/or other relevant aspects of securing new or altered content." ('193 262:21) - Function: "Importantly, VDE securely and flexibly supports editing the content in, extracting content from, embedding content into, and otherwise shaping the content composition of, VDE content containers." ('193 297:9) - VDE also features fundamentally important capabilities for managing content that travels "across" the "information highway." These capabilities comprise a rights protection solution that serves all electronic community members. These members include content creators and distributors, financial service providers, end-users, and others. VDE is the first general purpose, configurable, transaction control/rights protection solution for users of computers, other electronic appliances, networks, and the information highway." ('193 2:27) - VDE provides a unified solution that allows all content creators, providers, and users to employ the same electronic rights protection solution. ('193 5:17) - "Since different groups of components can be put together for different applications, the present invention can provide electronic control information for a wide variety of different products and markets. This means the present invention can provide a "unified," efficient, secure, and cost-effective system for electronic commerce and data security. This allows VDE to serve as a single standard for electronic rights protection, data security, and electronic currency and banking." ('193 7:6) - "Employing VDE as a general purpose electronic transaction/distribution control system allows users to maintain a single transaction management control arrangement on each of their computers, networks, communication nodes, and/or other electronic appliances. Such a general purpose system can serve the needs of many electronic transaction management applications without requiring distinct, different installations for different purposes. As a result, users of VDE can avoid the confusion and expense and other inefficiencies of different, limited purpose transaction control applications for each different content and/or business model. For example, VDE allows content creators to use the same VDE foundation control arrangement for both content authoring and for licensing content from other content creators for inclusion into their products or for other use. Clearinghouses, distributors, content creators, and other VDE users can all interact, both with the applications running on their VDE installations, and with each other, in an entirely consistent manner, using and reusing (largely transparently) the same distributed tools, mechanisms, and consistent user interfaces, regardless of the type of VDE activity." ('193 11:38) - An objective of VDE is supporting a transaction/distribution control standard. ('193 55:66) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad

Claim Term	MS Construction
	range of electronic appliances. The ability, for example, for control methods based on load modules to execute in very "small" and inexpensive secure sub-system environments, such as environments with very little read/write memory, while also being able to execute in large memory sub-systems that may be used in more expensive electronic appliances, supports consistency across many machines. This consistent VDE operating environment, including its control structures and container architecture, enables the use of standardized VDE content containers across a broad range of device types and host operating environments. Since VDE capabilities can be seamlessly integrated as extensions, additions, and/or modifications to fundamental capabilities of electronic appliances and host operating systems, VDE containers, content control information, and the VDE foundation will be able to work with many device types and these device types will be able to consistently and efficiently interpret and enforce VDE control information. ('193 21:43 34:26) - This rationalization stems from the reusability of control structures and user interfaces for a wide variety of transaction management related activities. As a result, content usage control, data security, information auditing, and electronic financial activities, can be supported with tools that are reusable, convenient, consistent, and familiar. In addition, a rational approach--a transaction/distribution control standard--allows all participants in VDE the same foundation set of hardware control and security, authoring, administration, and management tools to support widely varying types of information, business market model, and/or personal objectives ('193 11:26) - Because of the breadth of issues resolved by the present invention, it can provide the emerging "electronic highway" with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions. VDE's electronic transaction management mechanisms can enforce the electronic rights and agreements of all parties participating in widely varying business and data security models, and this can be efficiently achieved through a single VDE implementation within each VDE participant's electronic appliance. VDE supports widely varying business and/or data security models that can involve a broad range of participants at various "levels" of VDE content and/or content control information pathways of handling. Different content control and/or auditing models and agreements may be available on the same VDE installation. These models and agreements may control content in relationship to, for example, VDE installations and/or users in general; certain specific users, installations, classes and/or other groupings of installations and/or users; as well as to electronic content generally on a given installation, to specific properties, property portions, classes and/or other groupings of content.('193 17:22) - "the present invention's trusted/secure, universe wide, distributed transaction control and administration system." ('193 35:66) - "Commerce Utility Systems 90 are generalized and programmable..." ('712 67:7) - "Providers of "electronic currency" have also created protections for their type of content. These systems are not sufficiently adaptable, efficient, nor flexible enough to support the generalized use of electronic currency. Furthermore, they do not provide sophisticated auditing and control configuration capabilities. This means that current electronic currency tools lack the sophistication needed for many real- world financial business models. VDE provides means for anonymous currency and for "conditionally" anonymous currency, wherein currency related activities remain anonymous except under special circumstances." ('193 3:10) - "Traditional content control mechanisms often require users to purchase more electronic information than the user needs or desires. For example, infrequent users of shrink-wrapped software are required to purchase a program at the same price as frequent users, even though they may receive much less value from their less frequent use. Traditional systems do not scale cost according to the extent or character of usage and traditional systems can not attract potential customers who find that a fixed price is too high. Systems using traditional mechanisms are also not normally particularly secure. For example, shrink-wrapping does not prevent the constant illegal pirating of software once removed from either its physical or electronic package." ('193 5:50) - "Traditional electronic information rights protection systems are often inflexible and inefficient and

Claim Term	MS Construction
	may cause a content provider to choose costly distribution channels that increase a product's price. In general these mechanisms restrict product pricing, configuration, and marketing flexibility. These compromises are the result of techniques for controlling information which cannot accommodate both different content models and content models which reflect the many, varied requirements, such as content delivery strategies, of the model participants. This can limit a provider's ability to deliver sufficient overall value to justify a given product's cost in the eyes of many potential users. VDE allows content providers and distributors to create applications and distribution networks that reflect content providers' and users' preferred business models. It offers users a uniquely cost effective and feature rich system that supports the ways providers want to distribute information and the ways users want to use such information." ('193 5:36) - "VDE does not require electronic content providers and users to modify their business practices and personal preferences to conform to a metering and control application program that supports limited, largely fixed functionality [sic]. Furthermore, VDE permits participants to develop business models not feasible with non- electronic commerce, for example, involving detailed reporting of content usage information, large numbers of distinct transactions at hitherto infeasible low price points, "pass-along" control information that is enforced without involvement or advance knowledge of the participants, etc." ('193 9:67) - "VDE can further be used to enable commercially provided electronic content to be made available to users in user defined portions, rather than constraining the user to use portions of content that were "predetermined" by a content creator and/or other provider for billing purposes." ('193 11:66) - "The "usage map" concept provided by the preferred embodiment may be tied to the concept of "atomic elements." In the preferred embodiment, usage of an object 300 may be metered in terms of "atomic elements." In the preferred embodiment, an "atomic element" in the metering context defines a unit of usage that is "sufficiently significant" to be recorded in a meter. The definition of what constitutes an "atomic element" is determined by the creator of an object 300. For instance, a "byte" of information content contained in an object 300 could be defined as an "atomic element," or a record of a database could be defined as an "atomic element," or each chapter of an electronically published book could be defined as an "atomic element."" ('193 144:53) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention. VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, VDE includes features that: support dynamic user selection of information subsets of a VDE electronic information product (VDE controlled content). This contrasts with the constraints of having to use a few high level individual, pre-defined content provider information increments such as being required to select a whole information product or product section in order to acquire or otherwise use a portion of such product or section. VDE supports metering and usage control over a variety of increments (including "atomic" increments, and combinations of different increment types) that are selected ad hoc by a user and represent a collection of pre-identified one or more increments (such as one or more blocks of a preidentified nature, e.g., bytes, images, logically related blocks) that form a generally arbitrary, but logical to a user, content "deliverable." VDE control information (including budgeting, pricing and metering) can be configured so that it can specifically apply, as appropriate, to ad hoc selection of different, unanticipated variable user selected aggregations of information increments and pricing levels can be, at least in part, based on quantities and/or nature of mixed increment selections (for example, a certain quantity of certain text could mean associated images might be discounted by 15%; a greater quantity of text in the "mixed" increment selection might mean the images are discounted 20%). Such user selected aggregated information increments can reflect the actual requirements of a user for information and is more flexible than being limited to a single, or a few, high level, (e.g. product, document, database record) predetermined increments. Such high level increments may include quantities of information not desired by the user and as a result be more costly than the subset of information needed by the user if such a subset was available. In sum, the present invention allows information contained in electronic information products to be supplied according to user specification. Tailoring to user specification allows the present invention to provide

Claim Term	MS Construction
	the greatest value to users, which in turn will generate the greatest amount of electronic commerce activity. The user, for example, would be able to define an aggregation of content derived from various portions of an available content product, but which, as a deliverable for use by the user, is an entirely unique aggregated increment. The user may, for example, select certain numbers of bytes of information from various portions of an information product, such as a reference work, and copy them to disc in unencrypted form and be billed based on total number of bytes plus a surcharge on the number of "articles" that provided the bytes. A content provider might reasonably charge less for such a user defined information increment since the user does not require all of the content from all of the articles that contained desired information. ('193 21:43, 22:32) - Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.... Differing models for billing, auditing, and security can be applied to the same piece of electronic information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of electronic information control increments. ('193 21:43, 28:23)) - "The VDE templates, classes, and control structures are inherently flexible and configurable to reflect the breadth of information distribution and secure storage requirements, to allow for efficient adaptation into new industries as they evolve, and to reflect the evolution and/or change of an existing industry and/or business, as well as to support one or more groups of users who may be associated with certain permissions and/or budgets and object types. The flexibility of VDE templates, classes, and basic control structures is enhanced through the use of VDE aggregate and control methods which have a compound, conditional process impact on object control. Taken together, and employed at times with VDE administrative objects and VDE security arrangements and processes, the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment. Thus, the present invention fully supports the requirements and biases of content providers without forcing them to fit a predefined application model. It allows them to define the rights, control information, and flow of their content (and the return of audit information) through distribution channels." ('193 260:66) - VDE also extends usage control information to an arbitrary granular level (as opposed to a file based level provided by traditional operating systems) and provides flexible control information over any action associated with the information which can be described as a VDE controlled process." ('193 275:8) - "The situation is no better for processing documents within the context of ordinary computer and network systems. Although said systems can enforce access control information based on user identity, and can provide auditing mechanisms for tracking accesses to files, these are low-level mechanisms that do not permit tracking or controlling the flow of content. In such systems, because document content can be freely copied and manipulated, it is not possible to determine where document content has gone, or where it came from. In addition, because the control mechanisms in ordinary computer operating systems operate at a low level of abstraction, the entities they control are not necessarily the same as those that are manipulated by users. This particularly causes audit trails to be cluttered with voluminous information describing uninteresting activities." ('193 281:27) - "Importantly, VDE securely and flexibly supports editing the content in, extracting content from, embedding content into, and otherwise shaping the content composition of, VDE content containers." ('193 297:9) - "The InterTrust DigiBox container model allows and facilitates these and other different container uses. It facilitates detailed container customization for different uses, classes of use and/or users in order to meet different needs and business models. This customization ability is very important, particularly when used in conjunction with a general purpose, distributed rights management environment such as described in Ginter, et al. Such an environment calls for a practical optimization of customizability, including customizability and transparency for container models. This customization flexibility has a number of advantages, such as allowing optimization (e.g., maximum efficiency, minimum overhead) of the detailed container design for each particular application or circumstance so as to allow many different container designs for many different purposes (e.g., business models) to exist

Claim Term	MS Construction
	at the same time and be used by the rights control client (node) on a user electronic appliance such as a computer or entertainment device." ('861 2:49) - "The node and container model described above and in the Ginter et al. patent specification (along with similar other DigiBox/VDE (Virtual Distribution Environment) models) has nearly limitless flexibility." ('861 2:37) Such capabilities allow VDE supported product models to evolve by progressively reflecting requirements of "next" participants in an electronic commercial models." ('193 297:12) Extrinsic: VDE: VDE is the broad name given to a comprehensive system (algorithms, software, and hardware) that provides metering, securing, and administration tools for intellectual property. VDE stands for "Virtual Distribution Environment." (VDE ROI DEVICE v1.0a 9 Feb 1994, IT00008570) Virtual: Pertaining to a functional unit that appears to be real, but whose functions are accomplished by other means.(IBM) Environment: 1. The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. 2. In computer security, those factors, both internal and external, of an ADP system that help to define the risks associated with its operation (Longley) Environment: See InterTrust node: A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment.* (ITG, 8/21/95, IT00032375, TD00068B) InterTrust Commerce Architecture model: A model that defines a general-purpose distributed architecture for secure electronic commerce and digital rights management. The InterTrust Commerce Architecture model includes four key software elements: DigiBox secure containers, InterRights Point software with associated protected database, the InterTrust Transaction Authority Framework, and the InterTrust Deployment Manager. (ITG, 1997, ML00012A) VDE is a system using secure computing technology to enforce a chain of handling and control representing the rights of interested parties. (ITG, 3/7/1995, IT00709616) (see footnote 2) Virtual Distribution Environment (VDE): A set of components that protects content and enforces rights associated with content. (ITG, 3/7/1995, IT00709620, see footnote 2) Virtual Distribution Environment: or "VDE" shall mean a system which guarantees: (I) that the content creators, publishers, and/or distributors of information receive agreed upon fees for the use of, and/or records of the use of, electronic content; and/or (ii) that stored and/or distributed information will be used only in authorized ways. More particularly, VDE relates to systems for applying controls to, and controlling and/or auditing use of, electronically stored and/or disseminated information. [License Agreement, National Semiconductor and EPR, 3/18/94, Exhibit 12 to IT 30(b)(6)) IT0001689-96, IT0709785 (VDE on a Page), IT000202-29
'193:1	"The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
receiving a digital file including music	Intrinsic: - "Moreover, when any new VDE object 300 arrives at an electronic appliance 600, the electronic appliance must "register" the object within object registry 450 so that it can be accessed." ('193 153:56) - "FIGS. 114A and 114B show an example process 4600 for receiving an item. In this example,

Claim Term	MS Construction
	electronic appliance 600 that has received an electronic object 300 may first generate a notification to PPE 650 that the container has arrived (FIG. 114A, block 4602). PPE 650 may, in response, use the dynamic user interaction techniques discussed above to interact with and authenticate the recipient in accordance with the electronic controls 4078 within the received object 300 (FIG. 114A block 4603; authentication routine shown in FIG. 111). Intended recipient 4056 may be given an option of accepting or declining delivery of the object (FIG. 114A, block 4604). If intended recipient 4056 accepts the item, appliance may store the container 302 locally (FIG. 114A, block 4606) and then generate a "register object" event for processing by PPE 650.". - while grandparent ('107) did not refer to fax transmission or physical mail, it did recite that the delivery means could be by "physical storage media" or by transferring "physical things" ('193 3:26, 5:4, 14:21, 18:10, 127:6, 242:32) "In this example, the trusted electronic go-between between 4700 receives notification that the electronic container 302 has arrived (FIG. 121, block 4752), may store the container locally (FIG. 121, block 4754), and opens and authenticates the container and its contents (FIG. 121, block 4756). The trusted electonic go-between 4700 may then, if necessary, obtain and locally register any method/rules required to intract with secure container 302 (FIG. 121, block 4758)." Extrinsic:
a budget specifying the number of copies which can be made of said digital file	Intrinsic: - For example, content control information for a given piece of content may be stipulated as senior information and therefore not changeable, might be put in place by a content creator and might stipulate that national distributors of a given piece of their content may be permitted to make 100,000 copies per calendar quarter, so long as such copies are provided to bonfire end-users, but may pass only a single copy of such content to a local retailers and the control information limits such a retailer to making no more than 1,000 copies per month for retail sales to end-users. In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). ('193 48:19) - "storing a first digital file and a first control in a first secure container, said first control constituting a first budget which governs the number of copies which may be made of said first digital file or a portion of said first digital file while said first digital file is contained in said first secure container," ('193 claim 60) - "A certain content provider might, for example, require metering the number of copies made for distribution to employees of a given software program (a portion of the program might be maintained in encrypted form and require the presence of a VDE installation to run). This would require the execution of a metering method for copying of the property each time a copy was made for another employee." ('193 20:36) - For example, in the earlier example of a user with a desktop and a notebook computer, a provider may allow a user to make copies of information necessary to enable the notebook computer based on information present in the desktop computer, but not allow any further copies of said information to be made by the notebook VDE node. In this example, the distribution control structure described earlier would continue to exist on the desktop computer, but the copies of the enabling information passed to the notebook computer would lack the required distribution control structure to perform distribution from the notebook computer. Similarly, a distribution control structure may be provided by a content provider to a content provider who is a distributor in which a control structure would enable a certain number of copies to be made of a VDE content container object along with associated copies of permissions records, but the permissions records would be altered (as per specification of the content provider, for example) so as not to allow end-users who received distributor created copies from making further copies for distribution to other VDE nodes.('193 264:29) - "Similarly, a distribution control structure may be provided ... so as not to allow end-users who received distributor created copies from making further copies for distribution to other VDE nodes."

Claim Term	MS Construction
	('193 264:40) - SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. ('193 59:48) - " Secure container 302 may also contain an electronic, digital control structure 4078. This control structure 4078 (which could also be delivered independently in another container 302 different from the one carrying the image 4068I and/or the data 4068D) may contain important information controlling use of container 302. For example, controls 4078 may specify who can open container 302 and under what conditions the container can be opened. Controls 4078 might also specify who, if anyone, object 300 can be passed on to. As another example, controls 4078 might specify restrictions on how the image 4068I and/or data 4068D can be used (e.g., to allow the recipient to view but not change the image and/or data as one example). The detailed nature of control structure 4078 is described in connection, for example, with FIGS. 11D-11J ; FIG. 15 ; FIGS. 17-26B; and FIGS. 41A-61 ." ('683 25:62)"Many objects 300 that are distributed by physical media and/or by "out of channel" means (e.g., redistributed after receipt by a customer to another customer) might not include key blocks 810 in the same object 300 that is used to transport the content protected by the key blocks. This is because VDE objects may contain data that can be electronically copied outside the confines of a VDE node. If the content is encrypted, the copies will also be encrypted and the copier cannot gain access to the content unless she has the appropriate decryption key(s)." ('193 128:66) Although block 1262 includes encrypted summary services information on the back up, it preferably does not include SPU device private keys, shared keys, SPU code and other internal security information to prevent this information from ever becoming available to users even in encrypted form. ('193 166:59) Extrinsic:
controlling the copies made of said digital file	See above.
determining whether said digital file may be copied and stored on a second device based on at least said copy control	Intrinsic: - "Similarly, a distribution control structure may be provided ... so as not to allow end-users who received distributor created copies from making further copies for distribution to other VDE nodes." ('193 264:40) - "As mentioned above, traveling objects enable objects 300 to be distributed "Out-Of-Channel;" that is, the object may be distributed by an unauthorized or not explicitly authorized individual to another individual. "Out of channel" includes paths of distribution that allow, for example, a user to directly redistribute an object to another individual. For example, an object provider might allow users to redistribute copies of an object to their friends and associates (for example by physical delivery of storage media or by delivery over a computer network) such that if a friend or associate satisfies any certain criteria required for use of said object, he may do so." ('193 131:53) - "In some cases, the extract rights require an exact copy of the PERC 808 associated with the original object (or a PERC included for this purpose) to be placed in the new (destination) container ("no" exit to decision block 2096)." ('193 194:47) - "Metering, billing, and budgeting can allow a provider to enable and limit the copying of a permissions record 808." ('193 263:54) - "In some circumstances, it may be desirable for a provider to control how administrative processes are performed. The provider may choose to include in distribution records stored in secure database 610 information for use in conjunction with a component assembly 690 that controls and specifies, for example, how processing for a given event in relation to a given method and/or record should be performed. For example, if a provider wishes to allow a user to make copies of a permissions record

Claim Term	MS Construction
	808, she may want to alter the permissions record internally. For example, in the earlier example of a user with a desktop and a notebook computer, a provider may allow a user to make copies of information necessary to enable the notebook computer based on information present in the desktop computer, but not allow any further copies of said information to be made by the notebook VDE node. In this example, the distribution control structure described earlier would continue to exist on the desktop computer, but the copies of the enabling information passed to the notebook computer would lack the required distribution control structure to perform distribution from the notebook computer. Similarly, a distribution control structure may be provided by a content provider to a content provider who is a distributor in which a control structure would enable a certain number of copies to be made of a VDE content container object along with associated copies of permissions records, but the permissions records would be altered (as per specification of the content provider, for example) so as not to allow end-users who received distributor created copies from making further copies for distribution to other VDE nodes." ('193 264:20) "Transfer of ownership of a VDE object 300 is a special case in which all of the permissions and/or budgets for a VDE object are redistributed to a different PPE 650. Some VDE objects may require that all object-related information be delivered (e.g., it's possible to "sell" all rights to the object). However, some VDE objects 300 may prohibit such a transfer." ('193 220:41) Extrinsic:
if said copy control allows at least a portion of said digital file to be copied and stored on a second device	Intrinsic: - "Persistence of control includes the ability to extract information from a VDE container object by creating a new container whose contents are at least in part secured and that contains both the extracted content and at least a portion of the control information which control information of the original container and/or are at least in part produced by control information of the original container for this purpose and/or VDE installation control information stipulates should persist and/or control usage of content in the newly formed container." ('193 28:50) "enable a user to securely extract, through the use of the secure subsystem at the user's VDE installation, at least a portion of the content included within a VDE content container to produce a new, secure object (content container), such that the extracted information is maintained in a continually secure manner through the extraction process. Formation of the new VDE container containing such extracted content shall result in control information consistent with, or specified by, the source VDE content container, and/or local VDE installation secure subsystem as appropriate, content control information. Relevant control information, such as security and administrative information, derived, at least in part, from the parent (source) object's control information, will normally be automatically inserted into a new VDE content container object containing extracted VDE content. This process typically occurs under the control framework of a parent object and/or VDE installation control information executing at the user's VDE installation secure subsystem (with, for example, at least a portion of this inserted control information being stored securely in encrypted form in one or more permissions records)." ('193 31:66) Extrinsic:
copying at least a portion of said digital file	Intrinsic: "Usage map meters are thus an efficient means for referencing prior usage. They may be used to enable certain VDE related security functions such as testing for contiguousness (including relative contiguousness), logical relatedness (including relative logical relatedness), usage randomization, and other usage patterns. For example, the degree or character of the "randomness" of content usage by a user might serve as a potential indicator of attempts to circumvent VDE content budget limitations. A user or groups of users might employ multiple sessions to extract content in a manner which does not violate contiguousness, logical relatedness or quantity limitations, but which nevertheless enables reconstruction of a material portion or all of a given, valuable unit of content. Usage maps can be

Claim Term	MS Construction
	analyzed to determine other patterns of usage for pricing such as, for example, quantity discounting after usage of a certain quantity of any or certain atomic units, or for enabling a user to reaccess an object for which the user previously paid for unlimited accesses (or unlimited accesses over a certain time duration). Other useful analyses might include discounting for a given atomic unit for a plurality of uses." ('193 146:54) Extrinsic:
transferring at least a portion of said digital file to a second device	Intrinsic: - "In this case, these users may still be able to transfer some or all usage rights to another electronic appliance 600, and/or they may be permitted to move some of their rights to another electronic appliance, if such transferring and/or moving is permitted by the usage permissions received from the repository 200g." ('193 317:12) - "A result of processing the distribute event within the BUDGET method might be a secure communication (1454) between VDE nodes 102 and 106 by which a budget granting use and redistribute rights to the distributor 106 may be transferred from the creator 102 to the distributor." ('193 173:1) "VDE securely managed content (e.g. through the use of a VDE aware application or operating system having extraction capability) may be identified for extraction from each of one or more locations within one or more VDE content containers and may then be securely embedded into a new or existing VDE content container through processes executing VDE controls in a secure subsystem PPE 650." ('193 301:26) Extrinsic:
storing said digital file	See above.
'193:11	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
receiving a digital file	See above.
determining whether said digital file may be copied and stored on a second device based on said first control	See above.
identifying said second device	See above.
whether said first control allows	See above.

Claim Term	MS Construction
transfer of said copied file to said second device	
said determination based at least in part on the features present at the device	Intrinsic: - "The software-based tamper resistant barrier 674 provided by HPE 655 may be provided, for example, by: ... using a map of defects on a storage device (e.g., a hard disk, memory card, etc.) to form internal test values to impede moving and/or copying HPE 655 to other electronic appliances 600" ('193 80:40) "The degree of trustedness of a VDE arrangement will be primarily based on whether hardware SPUs are employed at participant location secure subsystems and the effectiveness of the SPU hardware security architecture, software security techniques when an SPU is emulated in software, and the encryption algorithm(s) and keys that are employed for securing content, control information, communications, and access to VDE node (VDE installation) secure subsystems." ('193 45:52) - "Independent claim 122 recites "determining step including identifying said second device and determining whether said first control allows transfer of said copied file to said device, said determination based at least in part on the features present at the device to which said copied file is to be transferred" which distinguishes over Löfberg which provides for determination of the identification of a second device (the user station) but dies [sic] not provide for basing the determination at least in part on the features present at the device to which the copied file is to be transferred." "At the terminal TERM the personal data carrier ID is used for the input of customer identification information, for example an account number or a corresponding information. Simultaneously, the time of rent and a programme identification information is supplied to the terminal." (Löfberg, U.S. Pat. No. 4,595,950, 12:51-56) 09/208,017 ('193), Examiner's Supplemental Notice of Allowability, 11/06/00, p. 2 (MSI026638) Extrinsic:
if said first control allows at least a portion of said digital file to be copied and stored on a second device	See above.
copying at least a portion of said digital file	See above.
transferring at least a portion of said digital file to a second device	See above.
storing said digital file	See above.
'193:15	"The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2

Claim Term	MS Construction
	See "Virtual Distribution Environment" above.
receiving a digital file	See above.
an authentication step comprising:	Intrinsic: "The secure subsystems at said user nodes utilize a protocol that establishes and authenticates each node's and/or participant's identity" ('193 12:35) Extrinsic:
accessing at least one identifier associated with a first device or with a user of said first device	Intrinsic: - "a stipulation that the traveling object may be used on certain one or more installations or installation classes or users or user classes where classes correspond to a specific subset of installations or users who are represented by a predefined class identifiers stored in a secure database 610" ('193 131:40) - "Thus, if the user had a VDE node, the user might be able to use the traveling object ... if he or his VDE node belonged to a specially authorized group of users or installations" ('193 132:13) - "A traveling object might register its user within itself and thereafter only be useable by that one user." ('193 133:43) - "Administrative objects, for example, may increase or otherwise adjust budgets and/or permissions of the receiving VDE node to which the administrative object is being sent." ('193 135:21) - "This metering process may ... record the VDE node name, user name, associated object identification information, time, date, and/or other identification information. Some or all of this information can become part of audit information securely reported by a clearinghouse or distributor.... For each metered one or more permissions records (or set of records) that were created for a certain user (and/or VDE node) to manage use of certain one or more VDE object(s) and/or to manage the creation of VDE object audit reports, it may be desirable that an auditor receive corresponding audit information incorporated into an, at least in part, encrypted audit report." ('193 273:58) - "provide very flexible and extensible user identification according to individuals, installations, by groups such as classes" ('193 25:31) "During the same or different communication session, the terminal could similarly, securely communicate back to the portable appliance 2600 VDE secure subsystem details as to the retail transaction (for example, what was purchased and price, the retail establishment's digital signature, the retail terminal's identifier, tax related information, etc.)." ('193 233:35) Extrinsic: "User Authentication: The [Database Management System] can require rigrous user authentication. For example, a DBMS might require a user to pass both specific password and time-of-day checks." (Pfleeger, p.307)
determining whether said identifier is associated with a device and/or user authorized to store said digital file	See above.
storing said digital file in a first secure memory of said first device, but	Intrinsic: Claims 91 and 132, as added with this Preliminary Amendment "91. A method comprising: receiving a digital file;

Claim Term	MS Construction
only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized	storing said digital file in a first secure memory of a first device; storing information associated with said digital file in a secure database stored on said first device, said information including at least one control; determining whether said digital file may be copied and stored on a second device based on said at least one control; if said at least one control allows at least a portion of said digital file to be copied and stored on a second device, copying at least a portion of said digital file; transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output; storing said digital file in said memory of said second device; and rendering said digital file through said output." "132. A method as in claim 91, further comprising: an authentication step occurring prior to said step of storing said digital file in said memory of said first device, said authentication step comprising: accessing at least one identifier associated with said first device or with a user of said first device; determining whether said identifier is associated with a device and/or user authorized to store said digital file; and proceeding with said storing step if said device and/or user is so authorized, but not proceeding with said step if said device and/or user is not authorized." 09/208,017 ('193), Preliminary Amendment, 12/09/98, p. 1-2, 12 "Claims ... 132-134 ... are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims." 09/208,017 ('193), Office Action, 06/07/00, p. 4-5 - "132. (Amended) A method [as in claim 91, further] comprising: receiving a digital file; an authentication step [occurring prior to said step of storing said digital file in said memory of said first device, said authentication step] comprising: accessing at least one identifier associated with a [said] first device or with a user of said first device; and determining whether said identifier is associated with a device and/or user authorized to store said digital file; [and proceeding with said storing step]; storing said digital file in a first secure memory of said first device, but only [proceeding with said storing step] if said device and/or user is so authorized, but not proceeding with said storing [step] if said device and/or user is not authorized; storing information associated with said digital file in a secure database stored on said first device, said information including at least one control; determining whether said digital file may be copied and stored on a second device based on said at least one control; if said at least one control allows at least a portion of said digital file to be copied and stored on a second device, copying at least a portion of said digital file; transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output; storing said digital file in said memory of said second device; and rendering said digital file through said output." (pg. 5-6) "The examiner also objected to claims ... 132-134, ... as dependent upon a rejected base claim (OA, ¶5). With this Amendment, Applicants have amended the above-mentioned claims to an independent form including all the limitations of the rejected base claim and any intervening claims per the Examiner's suggestion."

Claim Term	MS Construction
	(pg. 22) 09/208,017 ('193), Amendment, 08/04/00, p. 5-6, 22 Extrinsic:
storing information associated with said digital file in a secure database stored on said first device, said information including at least one control	See above.
determining whether said digital file may be copied and stored on a second device based on said at least one control	See above.
if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,	See above.
copying at least a portion of said digital file	See above.
transferring at least a portion of said digital file to a second device	See above.
storing said digital file	See above.
'193:19	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
receiving a digital file at a first device	See above.

Claim Term	MS Construction
establishing communication between said first device and a clearinghouse located at a location remote from said first device	Intrinsic: "A usage clearinghouse 200c as described above in connection with FIG. 1A and/or as disclosed in the Shear et al. patent disclosure may be used to track the audit information based on event-driven or periodic reporting, for example. Audit records could be transmitted to a usage clearinghouse (or to a trusted go-between 4700) by an automatic call forwarding transmission, by a supplement call during transmission, by period update of audit information, by the maintenance of a constant communication line or open network pathway, etc." ('683 37:56) Extrinsic:
using said authorization information to gain access to or make at least one use of said first digital file	See above.
receiving a first control from said clearinghouse at said first device	See above.
storing said first digital file in a memory of said first device	See above.
using said first control to determine whether said first digital file may be copied and stored on a second device	See above.
if said first control allows at least a portion of said first digital file to be copied and stored on a second device	See above.
copying at least a portion of said first digital file	See above.
transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output	See above.
storing said first	See above.

Claim Term	MS Construction
digital file portion	
'683:2	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above. - Prosecution History of '683 Patent: "A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... claim 7 recites hardware and/or software used for transmission of secure containers to other apparatuses and/or for the receipt of secure containers from other apparatuses, see column 1, lines 18-24 and column 4, lines 58-69." 09/221,479 ('683), Office Action, 11/12/99, 4-5 (IT00065800-01) - Fischer, U.S. Pat. No. 5,412,717 : "Each terminal, A, B . . . N also includes a conventional IBM communications board (not shown) which when coupled to a conventional modem 6, 8, 10, respectively, permits the terminals to transmit and receive messages. Each terminal is capable of generating a message performing whatever digital signature operations may be required and transmitting the message to any of the other terminals connected to communications channel 12 (or a communications network (not shown), which may be connected to communications channel 12)." (4:58-69)
the first secure container having been received from a second apparatus	Intrinsic: - "Incoming administrative object manager 756 typically maintains records (in concert with SPE 503) in secure database 610 (e.g., receiving table 446) that record which objects have been received, objects expected for receipt, and other information related to received and/or expected objects." ('193 102:46) - REGISTER method 2400 in this "administrative response" mode may prime appropriate audit trails (blocks 2460, 2462), and then may unpack the received administrative object and write the associated register request(s) configuration information into the secure database (blocks 2464, 2466). REGISTER method 2400 may then retrieve the administrative request from the secure database and determine which response method to run to process the request (blocks 2468, 2470). If the user fails to provide sufficient information to register the object, REGISTER method 2400 may fail (blocks 2472, 2474). ('193 179:23) - "Referring to FIG. 110, appliance 600 may then deliver the secure container(s) 302 to the intended recipient 4056 and/or to trusted electronic go-between 4700 based upon the instructions of sender 4052 as now reflected in the electronic controls 4078 associated with the object 300 (FIG. 110, block 4514). Such delivery is preferably by way of electronic network 4058 (672), but may be performed by any convenient electronic means such as, for example, Internet, Electronic Mail or Electronic Mail Attachment, WEB Page Direct, Telephone, floppy disks, bar codes in a fax transmission, filled ovals on a form delivered through physical mail, or any other electronic means to provide contact with the intended recipient(s)." ('683 40:10) Extrinsic:
an aspect of access to or use of	See above.

Claim Term	MS Construction
the first secure container rule having been received from a third apparatus different from said second apparatus	Intrinsic: "[A]pplicants' independent claims ... require secure delivery of both first and second control items originating from someplace other than the appliance where they are used, at least in part, for controlling the same process, operation or the like. This feature in combination is not taught or suggested by Johnson and/or Rosen." 08/388,107, Amendment, 06/20/97, p. 23 (MSI028847) - "Appliance 600 may next, if necessary, obtain and locally register any methods, controls or other information required to manipulate object 300 or its contents (FIG. 115, block 4607B; see registration method shown in FIGS. 43a-d). For example, item 4054 may be delivered independently of an associated control set 4078, where the control set may only be partial, such that appliance 600 may require additional controls from permissioning agent 200f (see FIG. 1A and "rights and permissions clearing house" description in the copending Shear et al. patent disclosure) or other archive in order to use the item." ('683 41:4) - "Secure container 302 may also contain an electronic, digital control structure 4078. This control structure 4078 (which could also be delivered independently in another container 302 different from the one carrying the image 4068I and/or the data 4068D) may contain important information controlling use of container 302." ('683 25:62) Extrinsic:
hardware or software used for receiving and opening secure containers	Intrinsic: "Please ... add the following new claims: 7. A system including, ... hardware and/or software used for receiving and opening secure containers ...." 09/221,479 ('683), Preliminary Amendment, 12/28/98, p. 2 - "SPU 500 in this example is an integrated circuit ("IC") "chip" 504 including "hardware" 506 and "firmware" 508. SPU 500 connects to the rest of the electronic appliance through an "appliance link" 510. SPU "firmware" 508 in this example is "software" such as a "computer program(s)" "embedded" within chip 504. Firmware 508 makes the hardware 506 work. Hardware 506 preferably contains a processor to perform instructions specified by firmware 508. "Hardware" 506 also contains long-term and short-term memories to store information securely so it can't be tampered with. SPU 500 may also have a protected clock/calendar used for timing events. The SPU hardware 506 in this example may include special purpose electronic circuits that are specially designed to perform certain processes (such as "encryption" and "decryption") rapidly and efficiently." ('193 59:60) - "Referring to FIG. 110, appliance 600 may then deliver the secure container(s) 302 to the intended recipient 4056 and/or to trusted electronic go-between 4700 based upon the instructions of sender 4052 as now reflected in the electronic controls 4078 associated with the object 300 (FIG. 110, block 4514). Such delivery is preferably by way of electronic network 4058 (672), but may be performed by any convenient electronic means such as, for example, Internet, Electronic Mail or Electronic Mail Attachment, WEB Page Direct, Telephone, floppy disks, bar codes in a fax transmission, filled ovals on a form delivered through physical mail, or any other electronic means to provide contact with the intended recipient(s)." ('683 40:10) - while grandparent ('107) did not refer to fax transmission or physical mail, it did recite that the delivery means could be by "physical storage media" or by transferring "physical things" ('193, 3:28, 5:4, 14:21, 18:10, 53:33, 127:6, 245:32) - "Incoming administrative object manager 756 receives administrative objects from other VDE electronic appliances 600 via communications manager 776." ('193 102:42)

Claim Term	MS Construction
	- Trusted go-between 4700 might be authorized to register (but not open) the containers 302(1) it receives for later use as evidence in court 5016. ('683 52:35) 479.7: "hardware and or/ [sic, and/or] software" Extrinsic:
said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers	Intrinsic: "VDE object creation in the preferred embodiment employs VDE templates whose atomic elements represent at least in part modular control processes. Employing VDE creation software (in the preferred embodiment a GUI programming process) and VDE templates, users may create VDE objects 300 by, for example, partitioning the objects, placing "meta data" (e.g., author's name, creation date, etc.) into them, and assigning rights associated with them and/or object content to, for example, a publisher and/or content creator. When a object creator runs through this process, she normally will go through a content specification procedure which will request required data. The content specification process, when satisfied, may be proceed by, for example, inserting data into a template and encapsulating the content." ('193 259:37) Extrinsic:
protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus	Intrinsic: See "protected processing environment" for Prosecution History limitations. "Such documents may be handled by people (referred to as "users") and/or by computers operating on behalf of users." ('193 277:36)" Extrinsic:
hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container	Intrinsic: - Prosecution History of '683 Patent: "A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... The combination of the first rule and the rule associated with the secure container is discussed at column 17, lines 40-61." U.S. Pat. No. 5,412,717 17:40-51: "Thereafter, the program X's program authorizing information is combined, as appropriate, with the PAI associated with the PCB of the calling program, if any. This combined PAI, which may include multiple PAI's, is then stored in an area of storage which cannot generally be modified by the program and the address of the PAI is stored in the process control block (PCB) as indicated in field 156 of FIG. 5. Thus, if program X is called by a calling program, it is subject to all its own constraints as well as being combined in some way with the constraints of the calling program, which aggregate constraints are embodied into program X's PAI." "A permissions record 808 may include requirements associated with this control information in combination with other control information, or a separate permissions record 808 may be used." ('193 262:17) 09/221,479 ('683), Office Action, 11/12/99, 4-5 (IT00065800-01)

Claim Term	MS Construction
	- "The VDE content control architecture allows content control information (such as control information for governing content usage) to be shaped to conform to VDE control information requirements of multiple parties. Formulating such multiple party content control information normally involves securely deriving control information from control information securely contributed by parties who play a role in a content handling and control model (e.g. content creator(s), provider(s), user(s), clearinghouse(s), etc.). Multiple party control information may be necessary in order to combine multiple pieces of independently managed VDE content into a single VDE container object (particularly if such independently managed content pieces have differing, for example conflicting, content control information). Such secure combination of VDE managed pieces of content will frequently require VDE's ability to securely derive content control information which accommodates the control information requirements, including any combinatorial rules, of the respective VDE managed pieces of content and reflects an acceptable agreement between such plural control information sets." ('193 296:12) - "The role of go-between 4700 may, in some circumstances, be played by one of the participant's SPU's 500 (PPEs), since SPU (PPE) behavior is not under the user's control, but rather can be under the control of rules and controls provided by one or more other parties other than the user (although in many instances the user can contribute his or her own controls to operate in combination with controls contributed by other parties)." ('683 24:26) - "Many such load modules are inherently configurable, aggregatable, portable, and extensible and singularly, or in combination (along with associated data), run as control methods under the VDE transaction operating environment." ('193 25:48) - "A permissions record 808 may include requirements associated with this control information in combination with other control information, or a separate permissions record 808 may be used." ('193 262:17) - "Seniority of contributed control information, including resolution of conflicts between content control information submitted by multiple parties, is normally established by:..." ('193 46:30) - "This attribute of supporting multiple party securely, independently deliverable control information is fundamental to enabling electronic commerce, that is, defining of a content and/or appliance control information set that represents the requirements of a collection of independent parties such as content creators, other content providers, financial service providers, and/or users." ('193 84:10) - "A significant feature of VDE accommodates the many, varying distribution and other transaction variables by, in part, decomposing electronic commerce and data security functions into generalized capability modules executable within a secure hardware SPU and/or corresponding software subsystem and further allowing extensive flexibility in assembling, modifying, and/or replacing, such modules (e.g. load modules and/or methods) in applications run on a VDE installation foundation. This configurability and reconfigurability allows electronic commerce and data security participants to reflect their priorities and requirements through a process of iteratively shaping an evolving extended electronic agreement (electronic control model). This shaping can occur as content control information passes from one VDE participant to another and to the extent allowed by "in place" content control information. This process allows users of VDE to recast existing control information and/or add new control information as necessary (including the elimination of no longer required elements)." ('193 16:5) - "A significant facet of the present invention's ability to broadly support electronic commerce is its ability to securely manage independently delivered VDE component objects containing control information (normally in the form of VDE objects containing one or more methods, data, or load module VDE components). This independently delivered control information can be integrated with senior and other pre-existing content control information to securely form derived control information using the negotiation mechanisms of the present invention. All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used. This means that, for example, all load modules and any mediating data which are listed by the derived control information as required must be available and securely perform their required function." ('193 10:66) - "Embedding takes content that is already in a container and stores it (or the complete object) in another container directly and/or by reference, integrating the control information associated with existing content with those of the new content." ('193 194:24)

Claim Term	MS Construction
	- However, the EMBED method 2110 performs a slightly different function-it writes an object (or reference) into a destination container. Blocks 2112-2122 shown in FIG. 57b are similar to blocks 2082-2092 shown in FIG. 57a. At block 2124, EMBED method 2110 writes the source object into the destination container, and may at the same time extract or change the control information of the destination container. One alternative is to simply leave the control information of the destination container alone, and include the full set of control information associated with the object being embedded in addition to the original container control information. As an optimization, however, the preferred embodiment provides a technique whereby the control information associated with the object being embedded are "abstracted" and incorporated into the control information of the destination container. ('193 195:3) - Users of VDE may include content creators who apply content usage, usage reporting, and/or usage payment related control information to electronic content and/or appliances for users such as end-user organizations, individuals, and content and/or appliance distributors. ('193 9:40) - For example, in a VDE aware word processor application, a user may be able to "print" a document into a VDE content container object, applying specific control information by selecting from amongst a series of different menu templates for different purposes (for example, a confidential memo template for internal organization purposes may restrict the ability to "keep," that is to make an electronic copy of the memo). ('193 26:59) - '479 c. 7: "hardware and/or software used for" - "Collection of terms (a control set) define a contract associated with a specific right," ('193 245:56) - "securely combining said first and second controls to form a set of controls." ('107 pg. 733 claim 45) - "the right to use the content may be associated with two control sets. One control set may describe a fixed ("higher") price for using the content. Another control set may describe a fixed ("lower") price for using the content with additional content information and field specification requiring collection and return the user's personal information." ('193 246:50) - "Multiple party control information may be necessary in order to combine multiple pieces of independently managed VDE content into a single VDE container object (particularly if such independently managed content pieces have differing, for example, conflicting, content control information). Such secure combinations of VDE managed pieces of content will frequently require VDE's ability to securely derive content control information which accommodates the control information requirements, including any combinatorial rules, of the respective VDE managed pieces of content and reflects an acceptable agreement between such plural control information sets."('193 296:21) - "Control sets 914, in turn, each includes a control set header 916, a control method 918, and one or more require methods records 920." ('193 150:24) - "Each control set 914 contains as many required methods records 920 as necessary to satisfy all of the requirements of the creators and/or distributors for the exercise of a right." ('193 150:51) "Control sets 914 exist in two type in VDE 100: common required control sets which are given designations, "control sets 0" or "control set for right," and a set of control set options. "Control set 0" 902 contain a list of reuired methods that are common to all control set options, so that the common required methods do not have to be duplicated in each control set option. A "control set for right" ("CSR") 910 contain a similar list for control sets within a given right. "Control set 0" and any "control sets for rights" are thus, as mentioned above, optimizations; the same functionality fir the control set can be accomplished by listing all the common required methods in each control set option and omitting "control set 0" and any "controls set for rights." ('193 150:30) [see Fig. 26] - "Rights and permissions clearinghouses 400 may then distribute a new, combined control set 188ABC consistent with each of the individual control sets 188A, 188B, 188C—relieving he value chain participants form having to formulate any control sets other than the one they are particularly concerned about." ('712 190:14-18)

Claim Term	MS Construction
	- "May form an overall transaction control set from a number of discrete sub-control sets contributed, for example, by a number of different participants." ('712 234:12-15) "Transaction authority 700 also receives another control set 188X specifying how to link the various participants' control sets together into overall transactions processes with requirements and limitations (Figures 58A and 58B, block 752). The overall transaction control set 188Y specifies how to resolve conflicts between the sub-transaction control set 188 (1), 188 (N) provided by the individual participants (this could involve, for example, an electronic negotiation process 798 as shown in Figures 75A-76A of the Ginter et al. patent disclosure). The transaction authority 700 combines the participant's individual control sets – trying them together with additional logic create an overall transaction control superset 188Y (Figures 58A and 58B, block 752)." ('712 243:8-19) Extrinsic:
hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Intrinsic: - "Referring to FIG. 110, appliance 600 may then deliver the secure container(s) 302 to the intended recipient 4056 and/or to trusted electronic go-between 4700 based upon the instructions of sender 4052 as now reflected in the electronic controls 4078 associated with the object 300 (FIG. 110, block 4514). Such delivery is preferably by way of electronic network 4058 (672), but may be performed by any convenient electronic means such as, for example, Internet, Electronic Mail or Electronic Mail Attachment, WEB Page Direct, Telephone, floppy disks, bar codes in a fax transmission, filled ovals on a form delivered through physical mail, or any other electronic means to provide contact with the intended recipient(s)." ('683 40:10) - while grandparent ('107) did not refer to fax transmission or physical mail, it did recite that the delivery means could be by "physical storage media" or by transferring "physical things" ('193 3:28, 5:4, 14:21, 18:10, 53:33, 127:6, 245:32) - Those programs may communicate with the PPE 650 component of a user's electronic appliance 600 to make VDE-protected documents available for use while limiting the extent to which their contents may be copied, stored, viewed, modified, and/or transmitted and/or otherwise further distributed outside the specific electronic appliance. ('193 279:3) - Extrinsic:
'721:1	Intrinsic: USP 5,757,914 USP 4,930,703 "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2
digitally signing a first load module with a first digital signature designating the first load module for use by a first	Intrinsic: - "A hierarchy of assurance levels may be provided for different protected processing environment security levels. Load modules or other executables can be provided with digital signatures associated with particular assurance levels. Appliances assigned to particular assurance levels can protect themselves from executing load modules or other executables associated with different assurance levels. Different digital signatures and/or certificates may be used to distinguish between load modules or other executables intended for different assurance levels." ('721 6:16)

Claim Term	MS Construction
device class	- "Encryption can be used in combination with the assurance level scheme discussed above to ensure that load modules or other executables can be executed only in specific environments or types of environments. The secure way to ensure that a load module or other executable can't execute in a particular environment is to ensure that the environment doesn't have the key(s) necessary to decrypt it." ('721 6:63) - "A protected processing environment(s) of assurance level I protects itself (themselves) by executing only load modules 54 sealed with an assurance level I digital signature 106(I). Protected processing environment(s) 108 having an associated assurance level I is (are) securely issued a public key 124(I) that can "unlock" the level I digital signature. Similarly, a protected processing environment(s) of assurance level II protects itself (themselves) by executing only the same (or different) load module 54 sealed with a "Level II" digital signature 106(II). Such a protected processing environment 108 having an associated corresponding assurance level II possess a public key 124(II) used to "unlock" the level II digital signature. A protected processing environment(s) 108 of assurance level III protects itself (themselves) by executing only load modules 54 having a digital signature 106(III) for assurance level III. Such an assurance level III protected processing environment 108 possesses a corresponding assurance level 3 public key 124(III)." ('721 17:48) - "More specifically, a particular assurance level appliance 61 thus protects itself from using a load module 54 of a different assurance level. Digital signatures (and/or signature algorithms) 106 in this sense create the isolated "desert islands" shown--since they allow execution environments to protect themselves from "off island" load modules 54 of different assurance levels." ('721 19:61) "If a load module is encrypted differently for different assurance levels, and the keys and/or algorithms that are used to decrypt such load modules are only distributed to environments of the same assurance level, an additional measure of security is provided." ('721 20:7) Extrinsic:
digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class	Intrinsic: - "In one example, verifying authority 100 may digitally sign identical copies of load module 54 for use by different classes or "assurance levels" of electronic appliances 61." - "Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. Tamper resistant barriers may be used to protect this programming or other conditioning. The assurance levels described below are a measure or assessment of the effectiveness with which this programming or other conditioning is protected." - "For example, protected processing environments or other secure execution spaces that are more impervious to tampering (such as those providing a higher degree of physical security) may use an assurance level that isolates it from protected processing environments or other secure execution spaces that are relatively more susceptible to tampering (such as those constructed solely by software executing on a general purpose digital computer in a non-secure location)." ('721 6:34) - "The present invention may use a verifying authority and the digital signatures it provides to compartmentalize the different electronic appliances depending on their level of security (e.g., work factor or relative tamper resistance)." - "Assurance level I might be used for an electronic appliance(s) 61 whose protected processing environment 108 is based on software techniques that may be somewhat resistant to tampering. An example of an assurance level I electronic appliance 61A might be a general purpose personal computer that executes software to create protected processing environment 108. An assurance level II electronic appliance 61B may provide a protected processing environment 108 based on a hybrid of software security techniques and hardware-based security techniques. An example of an assurance level II electronic appliance 61B might be a general purpose personal computer equipped with a hardware

Claim Term	MS Construction
	integrated circuit secure processing unit ("SPU") that performs some secure processing outside of the SPU (see Ginter et al. patent disclosure FIG. 10 and associated text). Such a hybrid arrangement might be relatively more resistant to tampering than a software-only implementation. The assurance level III appliance 61C shown is a general purpose personal computer equipped with a hardware-based secure processing unit 132 providing and completely containing protected processing environment 108 (see Ginter et al. FIGS. 6 and 9 for example). A silicon-based special purpose integrated circuit security chip is relatively more tamper-resistant than implementations relying on software techniques for some or all of their tamper-resistance." "Assurance level in this example may be assigned to a particular protected processing environment 108 at initialization (e.g., at the factory in the case of hardware-based secure processing units). Assigning assurance level at initialization time facilitates the use of key management (e.g., secure key exchange protocols) to enforce isolation based on assurance level. For example, since establishment of assurance level is done at initialization time, rather than in the field in this example, the key exchange mechanism can be used to provide new keys (assuming an assurance level has been established correctly)." Extrinsic:
distributing the first load module for use by at least one device in the first device class	See above.
distributing the second load module for use by at least one device in the second device class	See above.
'721:34	Intrinsic: USP 5,757,914 USP 4,930,703 "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
arrangement within the first tamper resistant barrier	Intrinsic: An important part of VDE provided by the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other electronic appliance, or network. ('193 48:66) Extrinsic:
prevents the first secure execution space from executing the same executable	Intrinsic: "In accordance with this feature of the invention, verifying authority 100 supports all of these various categories of digital signatures, and system 50 uses key management to distribute the appropriate verification keys to different assurance level devices. For example, verifying authority 100 may digitally sign a particular load module 54 such that only hardware-only based server(s) 402(3) at

Claim Term	MS Construction
accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level	assurance level XI may authenticate it. This compartmentalization prevents any load module executable on hardware-only servers 402(3) from executing on any other assurance level appliance (for example, software- only protected processing environment based support service 404(1))." ('721 19:11) Extrinsic:
'861:58	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
creating a first secure container	Intrinsic: - "For example, the descriptive data structure may be used in a creation process 302. The creation process 302 may read the descriptive data structure and, in response, create an output file 400 with a predefined format such as, for example, a container 100 corresponding to a format described by the descriptive data structure 200." ('861 11:58; Fig. 3) - "The output of the layout tool 300 may be a descriptive data structure 200 in the form of, for example, a text file. A secure packaging process 302a may accept container specific data as an input, and it may also accept the descriptive data structure 200 as a read only input. The packager 302a could be based on a graphical user interface and/or it could be automated. The packager 302a packages the container specific data 314 into a secure container 100. It may also package descriptive data structure 200 into the same container 100 if desired." ('861 12:9, and see Fig. 4) - "Descriptive data structure 200 may provide encodings of other characteristics in the form of metadata that can also be used by application 506 during a process of creating, using or manipulating container 100." ('861 13:30) - "This invention relates to techniques for defining, creating, and manipulating rights management data structures." ('861 1:23) - "Therefore, the container creation and usage tools must themselves be secure in the sense that they must protect certain details about the container design." ('861 4:59) - "The above-referenced Ginter et al. patent specification describes, by way of non-exhaustive example, "templates" that can act as a set (or collection of sets) of control instructions and/or data for object control software. See, for example, the "Object Creation and Initial Control Structures," "Templates and Classes," and "object definition file," "information" method and "content" methods discussions in the Ginter et al. specification. The described templates are, in at least some examples, capable of creating (and/or modifying) objects in a process that interacts with user instructions and provided content to create an object." ('861 4:65) - "The DDS creation tool 800 (see FIG. 10A) may then package the resulting DDS 200 into a secure container 100 along with an associated object 830" ('861 19:62) - "In accordance with one aspect of how to advantageously use descriptive data structures in accordance with a preferred embodiment of this invention, a machine readable descriptive data structure may be created by a provider to describe the layout of the provider's particular rights management data structure(s) such as secure containers. These descriptive data structure ("DDS") templates may be used to create containers." ('861 6:24) - "Object construction stage 1230 may use information in object configuration file 1240 to assemble or modify a container. This process typically involves communicating a series of events to SPE 503 to create one or more PERCs 808, public headers, private headers, and to encrypt content, all for storage in the new object 300 (or within secure database 610 within records associated with the new object)."

Claim Term	MS Construction
	('193 103:47) - "The Internet Repository 3406 VDE containerizes, including encrypts, selected object content as it streams out of the Repository in response to an online, user request to download an object." ('193 313:33) - "The container manager 764 may, in cooperation with SPE 503, construct an object container 302 based at least in part on parameters about new object content or other information as specified by object configuration file 1240. Container manager 764 may then insert into the container 302 the content or other information (as encrypted by SPE 503) to be included in the new object. Container manager 764 may also insert appropriate permissions, rules and/or control information into the container 302 (this permissions, rules and/or control information may be defined at least in part by user interaction through object submittal manager 774, and may be processed at least in part by SPE 503 to create secure data control structures). Container manager 764 may then write the new object to object repository 687, and the user or the electronic appliance may "register" the new object by including appropriate information within secure database 610. " ('193 104:12) [see Fig. 12A] Extrinsic:
including or addressing . . . organization information . . . desired organization of a content section. . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container	Intrinsic: - "metadata fields 264 (which may be part of and/or referenced by the descriptive data structure)" ('861 14:20); "include or reference" ('861 15:21); advantages of referencing ('861 15:32-58); alternative to referencing is "explicitly include" ('861 15:59); "including or addressing" (861.58); "includes a reference to" (861.69); - " it may be useful to store the metadata in a secure container 100 separately from DDS 200" ('861 15:35) - FIG. 7 shows an example of how descriptive data structure 200 may be formatted. As mentioned above, descriptive data structure 200 may comprise a list such as a linked list. Each list entry 260(1), 260(2), . . . may include a number of data fields including, for example: an object name field 262, one or more metadata fields 264 (which may be part of and/or referenced by the descriptive data structure); and location information 266 (which may be used to help identify the corresponding information within the container data structure 100)." - "a descriptive data structure could serve as `instructions` that drive an automated packaging application for digital content and/or an automated reader of digital content such as display priorities and organization (e.g., order and/or layout)."('861 7:54); - "a DDS 200 could serve as the `instructions` that drive an automated packaging application for digital content or an automated reader of digital content." ('861 13:) - "In accordance with one example, the machine readable descriptive data structure provides a description that reflects and/or defines corresponding structure(s) within the rights management data structure. For example, the descriptive data structure may provide a recursive, hierarchical list that reflects and/or defines a corresponding recursive, hierarchical structure within the rights management data structure. ... descriptive data structure may directly and/or indirectly specify where, in an associated rights management data structure, corresponding defined data types may be found." ('721 5:56); - Issued claim 1: a first memory storing a descriptive data structure, said descriptive data structure including: information regarding a first organization of elements within a secure container, said information including: information on the organization of said elements within said secure container; and information on the location of at least some of said elements within said secure container; " Issued claim 16: "using said organization information to identify a specific portion of said first secure container content." (see c. 17-19 re. specific specific portions) - Issued claim 34: "a representation of the format of data contained in a first rights management data structure said representation including: element information contained within said first rights management data structure; and organization information regarding the organization of said elements within said first rights management data structure; and information relating to metadata, said metadata including"

Claim Term	MS Construction
	- Issued claim 45 (dependent from 34-44): "said information regarding elements contained within said first rights management data structure includes information relating to the location of at least one such element." - Issued claim 73: "said descriptive data structure organization information includes information specifying that said first secure container contents will include at least a title and a text section referred to by said title." - Issued claim 74: "said descriptive data structure organization information includes information specifying that said first secure container contents will include at least one advertisement." - Issued claim 75: "said descriptive data structure further includes information relating to the location at which said title, said text section and said advertisement should be stored in said first secure container." - Issued claim 76: "at least a portion of said descriptive data structure organization information includes information specifying fields relating to at least one atomic transaction" - "For example, the FIG. 2A example descriptive data structure headline definition 202a does not specify a particular headline (e.g., "Yankees Win the Pennant!"), but instead defines the location (for example, the logical or other offset address) within the container data structure 100a (as well as certain other characteristics) in which such headline information may reside." ('861 10:54); "layout "hints" and field definitions (e.g., text, text block, integer, file, image or other data type)." ('861 16:49) - "A method of creating a first secure container, said method including the following steps;" ('861 this claim 58) "Descriptive data structure 200 can, for example, tell application 506 to always display a certain field (e.g., the author or copyright field) and to never display other information (e.g., information that should be hidden from most users)." ('861 13:) Extrinsic:
at least in part determine specific information required to be included in said first secure container contents	Intrinsic: - "Descriptive data structure 200 may provide encodings of other characteristics in the form of metadata that can also be used by application 506 during a process of *creating*, using or manipulating container 100. The DDS 200 can be used to generate a software program to manipulate rights management structures. For example, a DDS 200 could serve as the `instructions` that drive an automated packaging application for digital content or an automated reader of digital content." ('861 13:30); - "such metadata may impose integrity or other constraints during the creation and/or usage process (e.g., "when you create an object, you must provide this information", or "when you display the object, you must display this information")." ('861 15:25); "many possible integrity constraints.... Required: ... Optional ... Required relationship ... Optional relationship ... Repetition" ('861 16:15); - " "construction type" metadata (upon object construction, the information is required; upon object construction, the object creation tool is to always or never prompt for the information)" ('861 16:41); The descriptive data structure can be used to generate one or more portions of software programs that manipulate rights management structures. For example, a descriptive data structure could serve as `instructions` that drive an automated packaging application for digital content and/or an automated reader of digital content such as display priorities and organization (e.g., order and/or layout)." ('861 7:51) "In use, electronic appliance 500 may access secure container 100 and--in accordance with rules 316—access the descriptive data structure 200 and content 102 it contains and provide it to application 506. The interpreter 508 within application 506 may, in turn, read and use the descriptive data structure 200." For example, suppose the application 506 wants to display the "headline" information within newspaper style content shown in FIG. 2A. Application 506 may ask interpreter 508 to provide it with information that will help it to locate, read, format and/or display this "headline" information." ('861 12:57)

Claim Term	MS Construction
	Extrinsic:
rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents	Intrinsic: Prosecution History of '861 Patent: "Claims [1,10,25,26] are rejected under 35 U.S.C. 102(b) as being clearly anticipated by the common and decades-old practice of using database schema to describe the structure of a database which requires password/identifications for access. ... Claims [1-17,25-26] are rejected under 35 U.S.C. 102(a) as being anticipated by Anderson et al (Anderson), USP 5,537,526, Method and Apparatus for Processing a Display Document Utilizing a System Level Document. The claims are rejected on the basis of the correspondence between the teachings of Anderson and the elements of the claims as follows: As to claim 1 (and 10), the TabstractModel 502 is a machine readable, abstract descriptive data structure which interoperates with Tmodels 506 (TM), and TmodelSurrogates 504 (TMS). ... These models are clearly data structures, and while they can be of many types, the data they manage can include restrictions that correspond to rights management." 08/805,804 ('861), Office Action, 06/25/98, p. 2-3 - "The rights management environment in which DigiBox.TM. containers are used allows commerce participants to associate rules with the digital information (content)." ('861 1:50) - "For example, a creator of content can package one or more pieces of digital information with a set of rules in a DigiBox secure container--such rules may be variably located in one or more containers and/or client control nodes--and send the container to a distributor. The distributor can add to and/or modify the rules in the container within the parameters allowed by the creator. The distributor can then distribute the container by any rule allowed (or not prohibited) means--for example, by communicating it over an electronic network such as the Internet. A consumer can download the container, and use the content according to the rules within the container. The container is opened and the rules enforced on the local computer or other InterTrust-aware appliance by software InterTrust calls an InterTrust Commerce Node. The consumer can forward the container (or a copy of it) to other consumers, who can (if the rules allow) use the content according to the same, differing, or other included rules--which rules apply being determined by user available rights, such as the users specific identification, including any class membership(s) (e.g., an automobile club or employment by a certain university). In accordance with such rules, usage and/or payment information can be collected by the node and sent to one or more clearinghouses for payment settlement and to convey usage information to those with rights to receive it." ('861 2:13) - "Descriptive data structure 200 may supply integrity constraints or rules that protect the integrity of corresponding content during use of and/or access to the content." ('861 12:2) - "For example, DDS 200 can specify that an article of a newspaper cannot be viewed without its headline being viewed. The corresponding integrity constraint can indicate the rule 'if there is an article, there must also be a headline'." ('861 16:2) "In this example, each target data block 801 includes rule (control) information. Different target data blocks 801 can provide different rule information for different target environments 850. The rule information may, for example, relate to operations (events) and/or consequences of application program functions 856 within the associated target environment 850 such as specifying:" ('861 18:33) Extrinsic:
'891:1	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2

Claim Term	MS Construction
	See "Virtual Distribution Environment" above.
resource processed in a secure operating environment at a first appliance	Intrinsic: - Prosecution History of Application 08/388,107 (issued at '891): "Please amend the remaining claims as follows: 15. (Amended) A method for [managing] using at least one resource [with] processed in a secure operating environment at a first appliance, said method comprising: securely receiving a first entity's control [from a first entity] at said first appliance, said first entity being located remotely from [external to] said operating environment and said first appliance; securely receiving a second entity's control [from a second entity] at said first appliance, said second entity being located remotely from [external to] said operating environment and said first appliance, said second entity being different from said first entity; and securely processing a data item at said first appliance, using at least one resource [, a data item associated with said first and second controls; and], including securely applying, at said first appliance through use of said at least one resource, said first entity's control and said second entity's control [controls] to [manage said resource for] govern use [with] of said data item." 08/388,107, Amendment, 06/20/97, p. 2 (MSI028825) Extrinsic:
securely receiving a first entity's control at said first appliance	See above.
securely receiving a second entity's control at said first appliance	See above.
securely processing a data item at said first appliance, using at least one resource	Intrinsic: "a protected processing environment, coupled to said communications arrangements, that: (a) securely processing, using at least one resource, a data item associated with said first and second controls, and (b) securely applies said first and second controls to manage said resources for use of said data item." (08/388,107 page 781 claim 75) Extrinsic:
securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item	Intrinsic: "Such secure combination of VDE manage pieces of content will frequently require VDE's ability to securely derive content control information which accommodates the control information requirements, including any combinational rules, of the respective VDE managed pieces of content and reflects an acceptable agreement between plural control information sets." (293:12 Extrinsic:
'900:155	Intrinsic: "The instant application is one of a series of applications which are all generally directed to a virtual

Claim Term	MS Construction
	distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 Prosecution History of '900: Claims 302, 321 and 322, as pending: "302. A virtual distribution environment comprising • a first host processing environment comprising • a central processing unit; • main memory operatively connected to said central processing unit; • mass storage operatively connected to said central processing unit and said main memory; • said mass storage storing tamper resistant software designed to be loaded into said main memory and executed by said central processing unit, said tamper resistant software comprising: • machine check programming which derives information from one or more aspects of said host processing environment, • one or more storage locations storing said information; and • integrity programming which • causes said machine check programming to derive said information, • compares said information to information previously stored in said one or more storage locations, and • generates an indication based on the result of said comparison. 321. A virtual distribution environment as in claim 302, • said virtual distribution environment further comprising programming which takes one or more actions based on the state of said indication. 322. A virtual distribution environment as in claim 321 in which said one or more actions includes at least temporarily halting further processing." (08/706,206 ('900), Amendment, 06/09/98, 92-93, 96, 96-97) "Claims ... 322-324, ... are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims." 08/706,206 ('900), Office Action, 08/27/98, p. 2 "322. A virtual distribution environment comprising • a first host processing environment comprising • a central processing unit; • main memory operatively connected to said central processing unit; • mass storage operatively connected to said central processing unit and said main memory; • said mass storage storing tamper resistant software designed to be loaded into said main memory and executed by said central processing unit, said tamper resistant software comprising: • machine check programming which derives information from one or more aspects of said host processing environment, • one or more storage locations storing said information; • integrity programming which o causes said machine check programming to derive said information, o compares said information to information previously stored in said one or more storage locations, and o generates an indication based on the result of said comparison; and • programming which takes one or more actions based on the state of said indication; • said one or more actions including at least temporarily halting further processing." (pg. 27-28) Remarks, "Applicants appreciate the indication that claims ... are allowed and that claims ... 322-324

Claim Term	MS Construction
	are objected to but would be allowable if rewritten into independent form. ... For purposes of expedition, applicants are cancelling the rejected claims without prejudice ..., and are rewriting objected to dependent claims into independent form." (pg. 42) 08/706,206 ('900), Amendment, 11/23/98, p. 27-28, 42
first host processing environment comprising	See above.
said mass storage storing tamper resistant software	See above.
designed to be loaded into said main memory and executed by said central processing unit	See above.
said tamper resistant software comprising: . . . one or more storage locations storing said information	Intrinsic: "Referring once again to FIG. 69B, the installed operational materials 3472 may be further customized for each instance by making random changes to reserved, unused portions of the operational materials (FIG. 69B, block 3470(6)). An example of this is shown in FIG. 69E. In this example, the operational materials 3472 include unused, embedded random data or code portions 3494." Extrinsic:
derives information from one or more aspects of said host processing environment,	Intrinsic: ('900 73:1 - 80: 6); ('900 230:55 - 233:34); ('900 235:28-244:15); Figs. 69A-N
one or more storage locations storing said information	Intrinsic: "Referring once again to FIG. 69B, the installed operational materials 3472 may be further customized for each instance by making random changes to reserved, unused portions of the operational materials (FIG. 69B, block 3470(6)). An example of this is shown in FIG. 69E. In this example, the operational materials 3472 include unused, embedded random data or code portions 3494."
information previously stored in said one or more storage locations	Intrinsic: See terms.
generates an indication based on the result of said comparison	See terms.
programming which takes one or more actions based on the state of said indication	Intrinsic: Claim 321, as pending: "321. A virtual distribution environment as in claim 302, said virtual distribution environment further comprising programming which takes one or more actions

Claim Term	MS Construction
	based on the state of said indication." 08/706,206 ('900), Amendment, 06/09/98, p. 96
at least temporarily halting further processing	See halting.
'912:8	"The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
identifying at least one aspect of an execution space required for use and/or execution of the load module	Intrinsic: "For each site, the manufacturer generates a site ID 2821 and list of site characteristics 2822." ('193 209:55)
said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security	Extrinsic: See generally processor identification field, memory maps, and address spaces. (Tanenbaum, A., Modern Operating Systems, MSI096004)
checking said record for validity prior to performing said executing step	Extrinsic: Validity Check: The process of analyzing data to determine whether it conforms to predetermined completeness and consistency parameters. (Microsoft Computer Dictionary, 3rd ed. 1997)

Claim Term	MS Construction
'912:35	"The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." 09/208,017 ('193), Examiner's Amendment, 08/04/00, p. 2 See "Virtual Distribution Environment" above.
received in a secure container	See terms.
said component assembly allowing access to or use of specified information	See terms.
said first component assembly specified by said first record	See terms.